

From: [Paul Stockton](#)  
To: [Joseph McClelland](#)  
Cc: [Schaffer, Matthew J.](#)  
Subject: Grid Security Emergencies  
Date: Thursday, August 30, 2018 10:12:07 AM  
Attachments: [ResilienceforGridSecurityEmergencies.pdf](#)

---

Joe, I hope that you and your family will have a terrific Labor Day! At long last, attached is the final version of my study on "[Resilience for Grid Security Emergencies: Opportunities for Industry-Government Collaboration](#)." It is probably too far back for you to remember, but when I first got the study going, you and your FERC colleagues hosted an incredibly valuable round table for Matt Shaffer and me to identify key issues to address. My thanks to you and all at FERC, and please pass along the study to anyone who might be interested. I also understand we will be on a panel together for the Harvard electric Policy Group meeting coming up in October. It will be a pleasure to support you on the ballet liens once again!

Best, Paul

**Paul Stockton**  
**Managing Director, Sonecon, LLC**  
**325 7<sup>th</sup> Street NW**  
**Suite 250**  
**Washington, D.C. 20004**  
**202-393-2228**  
**Cell: 703 945 6574**  
[pstockton@sonecon.com](mailto:pstockton@sonecon.com)

# RESILIENCE FOR **GRID SECURITY** EMERGENCIES

**Opportunities for Industry–Government Collaboration**

**National Security Perspective**



Paul N. Stockton



# **RESILIENCE FOR GRID SECURITY EMERGENCIES**

Opportunities for Industry–Government Collaboration

Paul N. Stockton



Copyright © 2018 The Johns Hopkins University Applied Physics Laboratory LLC. All Rights Reserved.

This National Security Perspective contains the best opinion of the author at time of issue. The views expressed in this study are solely those of the author and do not necessarily reflect the opinions, practices, policies, procedures, or recommendations of the US Department of Energy or any other US government agency or of JHU/APL sponsors.

Contents

Figures..... v

Summary .....vii

**Developing Emergency Orders under the FPA..... 1**

    Drafting Template Emergency Orders before Attacks Occur ..... 3

    Participants in Drafting and Implementing Emergency Orders ..... 5

    Goals and Specific Design Requirements for Developing Emergency Orders ..... 11

**Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies ..... 13**

    Threats That Can Trigger Grid Security Emergencies ..... 13

    Thresholds for Declaring Grid Security Emergencies ..... 17

    Data Sharing and Consultations with Industry .....25

**Grid Security Emergency Phases and Order Design Options ..... 28**

    Preattack Options.....29

    Extraordinary Measures when Attacks Are Occurring.....33

    Emergency Orders to Support Power Restoration.....35

**Additional Emergency Order Design Parameters and Supporting Initiatives ..... 38**

    Deterring and Defeating US Adversaries.....38

    Communications Requirements for Issuing and Employing Emergency Orders .....46

    The Deeper Value Proposition for Emergency Orders.....52

**Conclusions and Recommendations for Broader Progress ..... 58**

    Employing Additional Emergency Authorities for Cross-Sector Resilience.....59

    Extended Partnership Requirements within the United States and Abroad.....64

    Playing Defense in Cyberwarfare .....70

Bibliography .....75

Acknowledgments.....93

About the Author .....93



## Figures

Figure S-1. Grid Security Emergency Phases.....	viii
Figure 1. Stakeholders for Building Grid Security Emergency Resilience.....	10
Figure 2. ODNI Cyber Threat Framework.....	20
Figure 3. Elements of the Cyber Incident Severity Schema .....	21
Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies.....	26
Figure 5. Emergency Order Matrix: Examples of Order Designs .....	29
Figure 6. Categories for Protecting Defense Critical Electric Infrastructure .....	41
Figure 7. NERC Regional Entities across North America .....	67

**Figure credits:**

Figure 2: “The Cyber Threat Framework,” ODNI (Office of the Director of National Intelligence), n.d., <https://www.dni.gov/index.php/cyber-threat-framework>.

Figure 3: DHS (US Department of Homeland Security), *National Cyber Incident Response Plan* (Washington, DC: DHS, December 2016).

Figure 7: Information from NERC (North American Electric Reliability Corporation), <http://www.nerc.com/Pages/default.aspx>; figure reprinted from Susan Lee, Michael Moskowitz, and Jane Pinelis, *Quantifying Improbability: An Analysis of the Lloyd’s of London Business Blackout Cyber Attack Scenario*, National Security Report NSAD-R-18-027 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018).





## Summary

The US Congress has opened the door to novel strategies for defending the country's electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act (FPA) in December 2015, Congress granted the secretary of energy vast new authorities to use when the president declares a grid security emergency. Most important, the secretary can issue emergency orders to power companies to protect and restore grid reliability when attacks on their systems are "imminent" or under way.<sup>1</sup> The FPA is silent, however, on what the secretary might require companies to do and how such orders can bolster their emergency operations.

The onset of an attack would be the worst possible time to develop emergency orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid. They could then adjust such orders to fit the specific circumstances of an attack. Developing emergency orders in advance would also help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. Companies could then exercise their contingency plans to build preparedness for response operations and contribute to national security in unprecedented ways.

This report is structured to help the electricity subsector and Department of Energy (DOE) develop emergency orders to defend the grid against potentially catastrophic cyber and physical attacks. The report highlights the phases that grid security emergencies are likely to entail. It analyzes the requirements that emergency orders will need to meet for each phase, and how orders can supplement existing utility plans and capabilities to fill gaps in grid resilience. The report also examines how emergency orders can strengthen deterrence against grid attacks and help defeat adversaries if deterrence fails.

The president must declare a grid security emergency before the secretary of energy can issue emergency orders. However, the FPA offers only broad and potentially ambiguous criteria for making that determination, especially for attacks that are imminent. Such ambiguity is useful; the president should retain the flexibility to declare grid security emergencies in a wide range of circumstances. Nevertheless, policy makers may find it useful to establish more detailed criteria to support their internal deliberations. This report proposes options for them to consider, including criteria derived from the electric industry's requirements to preserve "adequate levels of reliability" against cascading blackouts and other multistate grid disruptions. The report also examines how industry and government agencies can refine their information sharing mechanisms to support the emergency declaration process.

Once the president makes such a declaration, grid security emergencies may roll out in three phases, each of which provides the basis for developing a distinct set of template emergency orders. Figure S-1 illustrates these phases. The first will occur if the president determines that an attack is imminent. A well-established basis already exists for developing preattack emergency orders. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions. Such operations might include staffing up emergency operations centers, prepositioning recovery personnel and supplies, increasing available generation to help manage grid instabilities, and taking other precautionary measures. A key advantage of many of these options is that utilities can carry them

---

<sup>1</sup> Fixing America's Surface Transportation Act, Public Law 114-94.

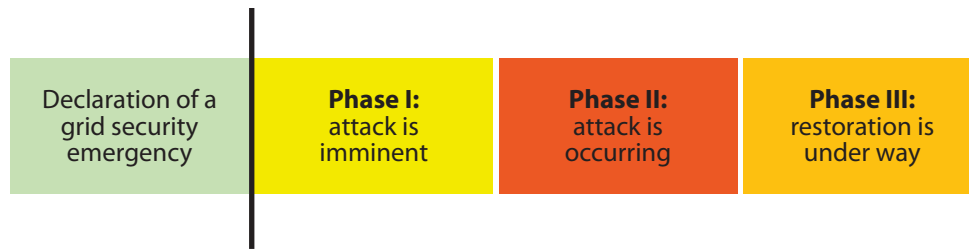


Figure S-1. Grid Security Emergency Phases

out without disrupting normal service; if the hurricane veers back to sea, utilities will have no regrets about having implemented them.

Power companies should help DOE develop equivalent “no-regrets” conservative operations to protect the grid against imminent cyber and physical attacks. A growing number of utilities are already adapting their existing plans for conservative operations to counter physical and cyber risks. These initiatives provide a strong foundation for developing emergency orders that will leverage best practices and help ensure that utilities will implement them on a consistent, nationwide basis. Moreover, because many of these conservative operations will inflict little or no disruption on normal grid service, they are ideal for protecting the grid when attacks are increasingly probable but not certain to occur. DOE and industry should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The next phase of grid security emergencies will occur when attacks are under way. Emergency orders for this phase can help utilities prevent power failures from cascading across the United States and prioritize the sustainment of electric service for military bases and facilities essential for public health (e.g., major regional hospitals and metropolitan water systems). As with conservative operations, existing electric industry plans and capabilities provide a strong basis for developing such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Orders for equivalent *extraordinary measures* could provide useful arrows in the quiver in grid security emergencies.

The final phase of grid security emergencies will commence as utilities begin restoring service to areas without power. Attacks that damage or destroy large numbers of high-voltage transformers and other difficult-to-replace grid components could create outages that darken major portions of the United States for many weeks, or even months. Power companies and DOE already have initiatives under way to meet this challenge. They should also collaborate to develop emergency orders to *support restoration*, which could facilitate the movement of replacement transformers and assist utilities in other strategically vital ways.

These grid security emergency phases could overlap. In particular, once power companies begin restoring power, adversaries may launch follow-on attacks that necessitate continued load shedding and other extraordinary measures to protect grid reliability. At the outset of an emergency, utilities should prepare to receive and implement orders across all emergency phases in an integrated way.

DOE and its industry partners should also design emergency orders to fill underlying gaps in preparedness for cyber and physical attacks. Power companies already have extensive plans and capabilities to protect and restore grid reliability against these threats, in part because mandatory reliability standards require them to do so. Grid owners and operators are also spring-loaded to employ emergency measures the moment they are

needed. Indeed, the North American Reliability Corporation can fine most major US power companies if they fail to implement emergency actions to protect grid reliability.<sup>2</sup> This robust industry preparedness begs the question: what added value can DOE emergency orders provide?

The most obvious benefit lies in the FPA's provisions for regulatory waivers and cost recovery. When grid owners and operators carry out emergency orders, they may have to violate environmental standards and other regulatory requirements. The FPA now protects entities from being punished for such violations if they occur while complying with emergency orders. The act also provides for the recovery of costs that companies will incur in implementing emergency orders. This report examines how further waiver and cost-recovery measures could reinforce preparedness for grid security emergencies.

Emergency orders can also help support national security in new and far-reaching ways. Russia, China, and other potential adversaries will not strike the grid simply to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to US defense installations responsible for deploying forces to the region, as well as to ports and other civilian infrastructure that supports force projection. Emergency orders can be designed to help deter—and, if necessary, defeat—such attacks. This report proposes specific options to do so, in support of the *National Security Strategy of the United States of America* and other sources of US policy guidance.

Some of these options will require harsh and politically contentious decisions on allocating power if adversaries severely disrupt the grid. Emergency orders for prioritized load shedding provide a case in point. To help deter attacks, grid owners and operators need the ability to sustain service to critical defense installations, including those responsible for conducting response operations against (and imposing costs on) potential attackers for however long a conflict may last. The ability to protect power flows to hospitals and other facilities vital for public health and safety will be valuable as well. However, if adversaries disrupt sufficient grid generation and transmission assets, sustaining reliable service to these installations may require utilities to curtail service to other customers. Government officials—and, ultimately, the president—should make such decisions and provide political top cover and liability protections for power companies that implement them.

Grid security emergencies will also create unprecedented challenges for government and industry to communicate with the American people. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Against a backdrop of fear and uncertainty, adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks. Adversaries may also disrupt the phone and internet-based communications systems utilities typically use to coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications playbooks to prepare for grid security emergencies, and they should make doing so a core component of the emergency order development process.

DOE and its industry and government partners will need to conduct intensive follow-on work to finalize the development of emergency orders and build utility-specific contingency plans to implement the orders in ways that account for accelerating structural changes in the electricity subsector. Their collaborative efforts will

---

<sup>2</sup> Bulk power system entities, including generation and high-voltage transmission companies, are subject to NERC's mandatory reliability standards and emergency orders under the FPA. For an analysis of applicability issues, see pages 5–10.

require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, as utilities and DOE tackle the immediate challenges of developing emergency orders, they should also explore broader opportunities to build preparedness for grid security emergencies. One such opportunity lies in integrating the use of emergency orders with other federal authorities. The secretary of energy can issue grid security emergency orders only to power companies. Increasingly, however, power generation depends on the flow of natural gas. Communications systems and other infrastructure sectors will also play critical roles in supporting power restoration. The secretary of energy and other federal leaders have additional authorities beyond section 215A of the FPA that can strengthen cross-sector resilience for grid security emergencies. However, achieving these benefits will require private and public sector leaders to preplan and exercise the coordinated use of these authorities, and to develop “whole-of-government” strategies to support infrastructure owners and operators.

Coordination with Canada could be valuable as well. The electric grids of the United States and Canada are deeply interconnected, and adversary-induced failures in one nation may rapidly cascade into the other. The secretary of energy does not have the authority to issue emergency orders to power companies in Canada (or in any other nation). Yet, significant opportunities exist to build on current reliability protections and emergency coordination mechanisms between US and Canadian utilities. The United States could also develop collaborative plans with Mexico as well as US allies in Europe and Asia.

In addition, DOE and its partners should explore further opportunities to help deter cyber attacks and defeat US adversaries if deterrence fails. The US *National Security Strategy* emphasizes that the United States needs to convince adversaries not only that they will suffer costly consequences if they attack but also that attacking will not accomplish the objectives they seek—in other words, achieve deterrence by denial. Yet, leading scholars of deterrence argue that deterrence by denial will be extraordinarily difficult to establish in cyberspace. Emergency orders and implementation plans can help meet these challenges by strengthening grid resilience in novel ways. Government agencies should also consider developing broader doctrine to “play defense” if cyberwarfare breaks out, and coordinate grid security emergency operations at home with measures to suppress adversary attacks at their source.

The foundational importance of the electric grid makes it a prime target for attack. As secretary of energy Richard Perry emphasizes, “America’s greatness depends on a reliable, resilient electric grid” that can power the economy, support national defense, and provide for the necessities of modern life.<sup>1</sup> To prevent adversaries from exploiting the United States’ dependence on the grid, the Department of Energy (DOE) and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter—and, if necessary, defeat—attacks on the grid.<sup>2</sup>

The FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the Fixing America’s Surface Transportation (FAST) Act amendments to the FPA, it greatly expanded the secretary of energy’s authority to issue emergency orders to grid owners and operators. Under section 215A of the act, “the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability” of critical electric infrastructure in a grid security emergency.<sup>3</sup> Before the secretary can issue those orders, the president

must first declare a grid security emergency when attacks on the grid are imminent or under way.<sup>4</sup>

However, legislators provided scant guidance on what the secretary might order power companies to do. DOE and its partners in the electricity subsector are now assessing which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats. This report supports their work by examining possible emergency orders and analyzing broader opportunities to strengthen resilience for grid security emergencies.

## Developing Emergency Orders under the FPA: Collaborative Opportunities, Fundamental Goals, and Overarching Design Requirements

The secretary of energy’s new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, “the nine most terrifying words in the English language are ‘I’m from the government and I’m here to help.’”<sup>5</sup> Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already taking steps to minimize such risks. Especially valuable, the department has incorporated industry recommendations on the process by which the secretary should issue emergency orders to utilities, and—“if practicable”—consult with industry before those orders are issued.<sup>6</sup> The next collaborative step should be to include power companies in

---

<sup>1</sup> Perry, letter to the FERC.

<sup>2</sup> The 2015 FAST Act amendments to the FPA provide the authority to undertake these efforts. Prior to 2015, section 202(c) of the FPA already authorized the secretary of energy to issue emergency orders to order “temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest.” That provision also specified that the secretary could exercise such powers “during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes.” See “DOE’s Use of Federal Power Act Emergency Authority,” DOE. The 2015 FAST Act amendments to the FPA gave the secretary further powers (mostly incorporated in section 215A of the act), which are the primary focus of this report.

<sup>3</sup> 16 U.S.C. § 824o, (b)(1).

---

<sup>4</sup> The analysis that follows examines the definition of such emergencies in the FPA and potential thresholds for declaring them.

<sup>5</sup> Reagan, “President’s News Conference.”

<sup>6</sup> DOE, “RIN 1901–AB40,” 1176; EEI, “Comments”; and Paradise et al., “ISO-RTO Council Comments.”



designing template emergency orders. Grid owners and operators have unequaled knowledge of their own infrastructure and operating procedures and extensive experience in employing emergency measures to protect and restore grid reliability.<sup>7</sup> They are well positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses—and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders would be most useful to help defend their systems and effectively supplement the emergency measures utilities would already be taking on their own. Utilities will also play a critical role in building company-specific plans to implement emergency orders, exercising those plans, and identifying remaining gaps to fill.

Strategic guidance from DOE and other government departments will be just as critical for designing emergency orders. Federal leadership will be essential to ensure that emergency orders help achieve overarching US security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing emergency orders to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.<sup>8</sup> Government officials can also shape emergency orders and supporting initiatives to help implement US cyber resilience strategies, including the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

(May 2017) and DOE's *Multiyear Plan for Energy Sector Cybersecurity* (March 2018).<sup>9</sup>

In addition, DOE will play critical a critical role in coordinating industry and government operations during grid security emergencies. The same congressional amendments that granted the secretary expansive new emergency authorities also specified that DOE shall be the federal government's "lead sector-specific agency for cybersecurity for the energy sector." As such, the secretary is responsible for collaborating with grid owners and operators, regulators, and other government agencies to help mitigate incidents and provide broader support to the energy sector.<sup>10</sup>

Federal incident response operational plans provide a broader framework for building these collaborative mechanisms. Presidential Policy Directive 41, *United States Cyber Incident Coordination* (July 2016), the *National Cyber Incident Response Plan* (December 2016), and the *National Response Framework* (June 2016) offer particularly useful guidance for building grid-specific coordination mechanisms.<sup>11</sup> DOE is also strengthening its own internal mechanisms and organizational structure to manage cyber incidents.<sup>12</sup> These changes further position the department to effectively collaborate with industry in developing and executing emergency orders.

<sup>9</sup> Trump, *Executive Order on Strengthening Cybersecurity*; and DOE, *Multiyear Plan*. See also Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*; and DHS, *Cybersecurity Strategy*.

<sup>10</sup> Fixing America's Surface Transportation Act, Public Law 114-94, 1779 (hereafter cited as FAST Act).

<sup>11</sup> Obama, *United States Cyber Incident Coordination*; DHS, *National Cyber Incident Response Plan*; and DHS, *National Response Framework*.

<sup>12</sup> DOE, *Multiyear Plan*, 28. DOE has also established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to "enable more coordinated preparedness and response to natural and man-made threats." See "Secretary of Energy Forms New Office," DOE.

<sup>7</sup> FERC and NERC, *Restoration and Recovery Plans*; FERC and NERC, *Planning Restoration Absent SCADA or EMS (PRASE)*; and FERC and NERC, *Recommended Study: Blackstart Resources Availability (BRAv)*. Additional BPS plans, exercises, and mandatory reliability standards are addressed in subsequent portions of the report.

<sup>8</sup> White House, *National Security Strategy*.

## Drafting Template Emergency Orders before Attacks Occur

The FPA specifies that before issuing emergency orders “the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action,” consult with appropriate power companies and other grid resilience stakeholders.<sup>13</sup> But opportunities for such consultations may be sharply limited. Adversaries may strike the grid with little or no warning. Moreover, when attacks are imminent or under way, rapidly issuing emergency orders may be crucial to help prevent cascading failures and other widespread disruptions. This imperative for speed could make consultations impractical.

To enable collaboration and minimize the risk that DOE will have to create orders amid the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, assistant secretary of energy for electricity delivery and energy reliability, stated in March 2018: “In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.”<sup>14</sup> Power companies and other electricity subsector organizations have also emphasized the need for industry and the government to jointly develop orders before adversaries strike.<sup>15</sup>

Such collaborative efforts should initially focus on creating *template orders*: orders that lay out the

basic types of actions that the secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act amendments’ potential value for the secretary to issue general orders to “protect and restore the reliability of the grid.” Vague, overly broad directives cannot provide an adequate basis for utilities to develop system-specific plans to implement them. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for “maximum generation” and increased reserve margins to more aggressive, far-reaching measures.<sup>16</sup> A key objective for such development efforts: provide a menu of agreed-upon options from which the secretary can choose as circumstances require, supported as much as possible by consultations with industry.

Developing emergency orders before attacks occur can help ensure that, as a minimalist goal, such orders will “do no harm.” By participating in the order design process, power companies can shape orders to account for system-specific engineering constraints and requirements for emergency operations. This industry input will be especially important because DOE has the authority to punish utilities for failing to comply with emergency orders, even if they are poorly designed. DOE’s grid security emergency rule specifies that “in accordance with available enforcement authorities, the secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order.”<sup>17</sup> If

<sup>13</sup> This includes the North American Electric Reliability Corporation (NERC) and its Electricity Information Sharing and Analysis Center (E-ISAC). 16 U.S.C. § 824o–1. See also the notice of proposed rulemaking and request for comment (DOE, “RIN 1901–AB40”).

<sup>14</sup> Walker, *Written Testimony*.

<sup>15</sup> See Joint Commenters, “Comments; and NASEO, “Comments.”

<sup>16</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual* 13, 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help “maintain reliable operation while meeting . . . unexpected outages of existing capacity.” See “M-1 Reserve Margin,” NERC.

<sup>17</sup> DOE, “RIN 1901–AB40,” 1182.



power companies find that an order is impossible to implement or is otherwise objectionable, they can ask DOE to reconsider it.<sup>18</sup> But adjudicating individual emergency orders amid a grid security emergency could delay time-critical actions. Instead, DOE should include industry in developing emergency orders from the start and resolve utility concerns before adversaries strike.

Preplanning to coordinate industry and government emergency operations will also be valuable. Power companies are already poised to take immediate emergency actions to protect grid reliability as circumstances require, regardless of whether the secretary issues emergency orders. It will be helpful to understand in advance how DOE can best align the issuance of such orders with industry-initiated actions. Once attacks are under way, preplanning for operational coordination will become still more important, especially if adversaries continue striking the grid and its supporting communications systems after their initial salvo.

If attacks do occur, Russia, China, or other potential adversaries will use country-specific tactics, techniques, and procedures to disrupt US infrastructure. Defending against those attacks will require tactical and operational responses that are similarly tailored to specific adversaries. Over time, it may be possible to develop (and protect adversaries from accessing) emergency orders that account for these individualized defensive requirements. US leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this report examines opportunities to do so.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders

should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high-voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military bases, regional hospitals, and other critical customers that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and identify opportunities to improve order design and execution. Training programs to prepare employees to carry out utility-specific implementation plans should also get under way as soon as possible. On a larger scale, utilities will also be able to exercise the implementation of template emergency orders within the framework of the Cyber Mutual Assistance (CMA) Program. This program enables over 140 utilities in the United States and Canada to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.<sup>19</sup> Exercises can help determine how best to align the issuance and implementation of emergency orders with these growing capabilities for mutual support.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the secretary of energy has the sole authority to issue emergency orders, the secretary may request input from senior DOE staffers

<sup>18</sup> DOE, "RIN 1901-AB40," 1181-1182.

<sup>19</sup> "ESCC's Cyber Mutual Assistance Program," ESCC.

on which orders will be most useful against specific types of attacks. The secretary may also need to brief the president and the National Security Council on proposed orders and their potential benefits. By developing orders and clarifying their respective advantages before adversaries strike, DOE and industry partners can facilitate such deliberations.

Over the longer term, industry and government leaders might structure their collaboration to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public-private and interagency coordination.<sup>20</sup> Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government-industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, to develop template emergency orders and contingency plans to implement them, power companies will need to conduct extensive operational and engineering studies and use enhanced modeling to understand the potential impact of such orders. The FAST Act amendments to the FPA provide no funding for such development efforts. Moreover, DOE and power companies are only the most obvious participants in the order design process. A wide array of other grid resilience and incident management stakeholders may also need to assist that process—including critical ones not mentioned in the FPA. Determining which specific public and private sector organizations should help shape template orders constitutes a critical first step in preparing for grid security emergencies.

## Participants in Drafting and Implementing Emergency Orders: The Bulk Power System and the Broader Electricity Subsector

An initial task in developing emergency orders will be to determine which components of the electricity subsector should participate in that effort. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>21</sup> The most obvious candidates for inclusion are the power companies that are subject to emergency orders. The FAST Act amendments to the FPA specify which components fall into that category. Chief among them are “any owner, use or operator of critical electric infrastructure or of defense critical electric infrastructure within the United States.”<sup>22</sup> The FPA also includes criteria to identify this infrastructure. Critical electric infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>23</sup> Defense critical electric infrastructure consists of grid components that serve facilities “critical to the defense of the United States” and that are vulnerable to the disruption of grid-provided power.<sup>24</sup>

However, Congress also narrowed the definition of critical electric infrastructure in a significant way. The FPA states that such infrastructure only includes assets that compose the bulk power system (BPS). BPS assets are those “facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation

<sup>20</sup> Danzig, *Catastrophic Bioterrorism*, 5–7; and Blue Ribbon Study Panel, *National Blueprint*, 13, 42–44.

<sup>21</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>22</sup> 16 U.S.C. § 824o–1, (b)(4)(c).

<sup>23</sup> 16 U.S.C. § 824o–1, (a)(2).

<sup>24</sup> 16 U.S.C. § 824o–1, (a)(4).

facilities needed to maintain transmission system reliability.”<sup>25</sup> These BPS generation and transmission assets provide synchronized power within the three interconnections that serve the entire United States and parts of Mexico and Canada.<sup>26</sup>

As defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.<sup>27</sup> That limitation creates a potential problem for executing emergency orders. Local distribution systems often provide the “last mile” of connectivity between transmission systems and military bases and other critical customers. As DOE and industry create template emergency orders and execution plans, it will be essential to integrate local distribution providers into that development process.

However, before examining these distribution-level issues, it will first be helpful to clarify the components of the BPS that are explicitly subject to emergency orders under the FPA (and are therefore key partners for DOE in designing them). The FPA states that the secretary of energy may issue emergency orders to the following the BPS “entities:”<sup>28</sup>

**The Electric Reliability Organization.** After blackouts cascaded across major portions of the United States in August 2003, Congress authorized the Federal Energy Regulatory Commission (FERC) to certify an electric reliability organization to develop and enforce, subject to FERC approval, mandatory

electric reliability standards for all users, owners, and operators of the US BPS.<sup>29</sup> FERC certified the North American Electric Reliability Council (NERC) as the first-ever electric reliability organization in July 2006. Renamed the North American Electric Reliability Corporation in 2007, it has served in that role since.<sup>30</sup> NERC’s mission is to ensure the reliability and security of the BPS in North America. As such, NERC is uniquely positioned to help DOE develop emergency orders, especially for attacks that could create cascading blackouts or other multistate disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a leading role for the electricity subsector in establishing situational awareness, incident management and coordination, and communication capabilities.<sup>31</sup> E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be vital for responding to grid security emergencies.

**Regional entities responsible for enforcing reliability standards for the BPS.**<sup>32</sup> NERC has delegated certain authorities to eight regional entities to monitor and enforce compliance with reliability standards.<sup>33</sup> While regional entities play major oversight roles, they do not directly operate the physical grid and would not, on their own, be positioned to execute emergency orders. However, they could help utilities and DOE and preplan for

<sup>25</sup> 16 U.S.C. § 824o, (a)(1).

<sup>26</sup> Interconnections are defined as the “geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control.” North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See NERC, *Glossary*.

<sup>27</sup> The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify “local” distribution. See 16 U.S.C. § 824o, (a).

<sup>28</sup> 16 U.S.C. § 824o–1, (b)(4).

<sup>29</sup> Energy Policy Act of 2005, Public Law 109-58. This does not include Alaska or Hawaii.

<sup>30</sup> NERC, *History*. For more information on NERC, see “About NERC,” NERC.

<sup>31</sup> “Electricity Information Sharing and Analysis Center,” NERC.

<sup>32</sup> DOE, “RIN 1901–AB40,” 1177. See also 16 U.S.C. § 824o, (a)(7).

<sup>33</sup> “Key Players,” NERC. In July 2017, however, one regional entity announced its intention to dissolve. FERC has approved the dissolution, effective July 2018. See FERC, *Order Granting Approvals* (163 FERC ¶ 61,094).

issuing regulatory waivers to BPS grid operators as they comply with emergency orders.

**Owners, users, and operators of critical electric infrastructure or defense critical electric infrastructure within the United States.**<sup>34</sup> Companies that own and operate generation and transmission assets will be among the most likely recipients of emergency orders and should play a critical role in designing them. Reliability coordinators will be similarly important. Reliability coordinators are the entities that constitute “the highest level of authority” for the reliable operation of the bulk electric system (BES).<sup>35</sup> They are also responsible for maintaining a “wide-area view” of the BES and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, reliability coordinators will be critical for designing, receiving, and implementing emergency orders to counter attacks that individual BPS owners and operators may not have the ability to defeat. Seven regional transmission organizations and independent system operators, most of which are registered as reliability coordinators, also help operate and ensure the reliability of the BES in many regions of the United States.<sup>36</sup> Accordingly, regional

transmission organizations and independent system operators will be essential to the design and execution of emergency orders.

### **Local Distribution Providers and Other Grid Resilience Stakeholders**

The 2015 FAST Act amendments to the FPA do not explicitly address the possible roles of local distribution systems in grid security emergencies. However, local distribution infrastructure is critical for overall resilience against cyber and physical attacks. Even if emergency orders help defeat attacks on BPS assets, adversaries may still be able to achieve catastrophic effects by striking multiple local distribution systems and thereby interrupting the flow of power from transmission systems to military bases, hospitals, and other end users. Local distribution systems may also need to help implement emergency orders issued to BPS entities. For example, if the secretary orders transmission systems to protect reliability by shedding load, yet at the same time sustain the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding. Holistic preparedness for grid security emergencies therefore requires engagement with local distribution systems.

These systems will also have strong incentives to participate in the emergency order planning process. Just as BPS entities rely on local distribution utilities, these utilities rely on generation, transmission, and higher-voltage distribution entities to serve end users. Local systems will also share the commitment of BPS entities to protect and rapidly restore service to defense installations and other critical customers. By integrating local distribution utilities

---

<sup>34</sup> The analysis that follows later in this section examines the definition of “users” of critical electric infrastructure and defense critical electric infrastructure.

<sup>35</sup> While the BPS broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the BES is a subset of the BPS that includes, with some exclusions, all transmission and real and reactive power sources at one hundred kilovolts or higher. As with the BPS definition, the BES definition excludes local distribution providers. For these definitions, as well as the definition of reliability coordinators, see NERC, *Glossary*. Consistent with the FPA and the authorities it provides for handling grid security emergencies, this report focuses on the application of emergency orders to BPS entities specifically.

<sup>36</sup> There are ten regional transmission organizations and independent system operators under NERC’s purview, though three operate exclusively in Canada. Regional transmission organizations and independent system operators are independent membership-based nonprofit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are

---

operated by individual utilities or utility holding companies. See “About 60% of U.S. Electric Power Supply Managed by RTOs,” US Energy Information Administration. Six of the seven regional transmission organizations/independent system operators operating in the US are also current reliability coordinators. See “Reliability Coordinators,” NERC.



into emergency order planning, these utilities will be able to participate in shaping template orders and implementation plans to help achieve their reliability goals when adversaries strike. Moreover, to the extent that local distribution companies may be subject to emergency orders, they may also benefit from the FPA's liability protections and cost-recovery provisions for actions taken to execute those orders.

DOE and other stakeholders may determine that the FPA already gives the secretary adequate authority to issue emergency orders to local distribution companies. The act states that emergency orders may apply to "any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure" within the United States.<sup>37</sup> The act, however, does not further define owners, users, and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the act.

Regardless of whether the secretary can issue orders to local distribution utilities, BPS entities should include them in building the contingency plans to implement emergency orders. This preplanning will be essential to strengthen comprehensive, end-to-end protection of grid reliability against attacks.

Many companies that own transmission assets also own distribution infrastructure. These utilities will find it relatively easy to include distribution assets in their emergency planning. Integrated response plans will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for "vertically integrated" utilities that own and operate assets for all three functions. However, many municipally owned electric utilities and rural electric cooperatives (including those that serve critical and defense critical electric infrastructure) are not part of vertically integrated companies. In US regions where generation, transmission,

and distribution systems exist as separate entities, additional engagement initiatives will be essential to implement emergency orders and sustain power to essential facilities.

Including state regulators and other state officials in these integrative efforts could offer additional benefits. State public utility commissions have primary regulatory jurisdiction over distribution systems.<sup>38</sup> The National Association of Regulatory Utility Commissioners, which represents state regulators nationwide, has focused growing attention on the need for prudent utility investments in cyber and physical resilience.<sup>39</sup> Commissioners in New Jersey and other states are also leading regulatory initiatives to bolster cyber resilience in their respective jurisdictions.<sup>40</sup> Emergency managers and National Guard leaders in a growing number of states are also building new mechanisms to coordinate with utilities in responding to cyber attacks. Adding such additional partners to help design emergency orders and plan for their implementation would complicate an already far-reaching engagement process. Nevertheless, incorporating perspectives from state commissioners and other officials would help advance comprehensive state-level preparedness for grid security emergencies.

### **Additional Partners for Engagement**

DOE and power companies will need to collaborate with a wider array of partners to develop and execute some potentially useful emergency orders, especially to support grid restoration. The final rule

---

<sup>37</sup> 16 U.S.C. § 824o, (b)(4)(a).

---

<sup>38</sup> The US Constitution, in most cases, allows federal regulation of private economic activity only for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See Lazar, *Electricity Regulation in the US*, 15.

<sup>39</sup> See NARUC, *Cybersecurity*; and NARUC, *Resolution on Physical Security*.

<sup>40</sup> State of New Jersey Board of Public Utilities, *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196).

on *Grid Security Emergency Orders: Procedures for Issuance* (hereinafter referred to as the grid security emergency rule) notes: “Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits” to expedite the restoration of power.<sup>41</sup> This includes traditional partners such as the Department of Homeland Security (DHS) and the Department of Defense (DOD). Still broader collaboration with government and private sector partners may be valuable for implementing emergency orders to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy large power transformers at substations across the United States, and these attacks cut off power to critical military bases, the secretary might order industry to prioritize the replacement of large power transformers at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program to provide for such replacements.<sup>42</sup> New industry-led organizations such as Grid Assurance,<sup>43</sup> as well as programs such as the Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) initiative, are further expanding the industry’s capacity to replace transformers and other equipment.<sup>44</sup> These efforts will be essential for preparing for grid security emergencies, especially as industry stocks and securely stores the full range of replacement transformer types and sizes that large-scale physical attacks may require.

However, power companies do not move large power transformers by themselves. They rely on railroad companies, barges, and heavy-haul trucking companies to help do so and have established a

Transformer Transportation Working Group under the ESCC to plan and coordinate transformer movement.<sup>45</sup> Exercises in the Spare Transformer Equipment Program now involve representation from transportation stakeholders. Yet, the FPA does not give the secretary authority to issue orders to transportation companies. In anticipation of orders for replacing transformers, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Preplanning with the US Department of Transportation (DOT), the Federal Emergency Management Agency (FEMA), and state governments to get contracts, permits, and regulatory waivers to expedite transformer movement will also be useful. In addition, advance coordination with emergency managers at all levels of government would help them mitigate the effects of rotating blackouts or other extraordinary measures on public health and safety.

DOE and the electricity subsector should consider expanding the geographic scope of these discussions as well. In defining the defense critical electric infrastructure that emergency orders can protect, Congress excluded grid assets in Alaska and Hawaii.<sup>46</sup> But both states are home to vital military installations, as are a number of US territories. The secretary also lacks the authority to issue emergency orders to Canadian utilities. Yet, US and Canadian electric systems are deeply integrated, and coordinated efforts to prevent instabilities in grid security emergencies could benefit both nations. Collaborations with NATO allies and other security partners in the face of major adversarial cyber campaigns could be valuable as well. The concluding section of this report examines the potential benefits of expanding grid

<sup>41</sup> DOE, “RIN 1901–AB40,” 1177.

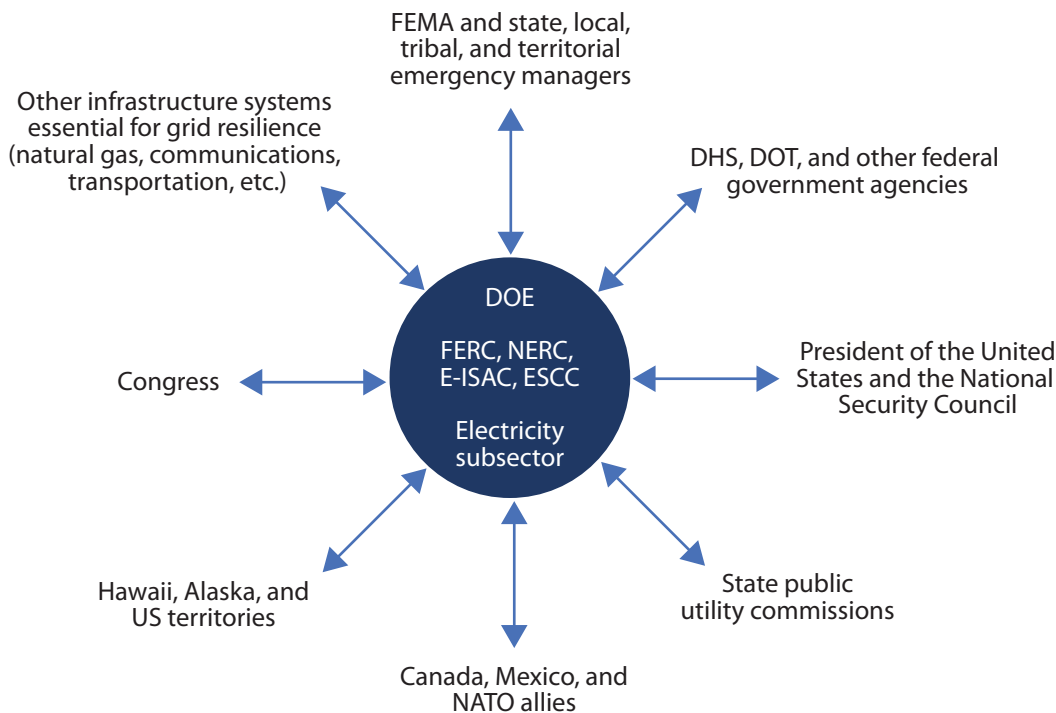
<sup>42</sup> See DOE, *Strategic Transformer Reserve*; and “Spare Transformers,” EEL.

<sup>43</sup> “Transmission Equipment Ready,” Grid Assurance.

<sup>44</sup> FERC, *Order Authorizing Acquisition and Disposition* (163 FERC ¶ 61,005), 10.

<sup>45</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>46</sup> 16 U.S.C. § 824o–1, (a)(4). The FPA’s section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).



**Figure 1. Stakeholders for Building Grid Security Emergency Resilience**

security emergency coordination within the United States and beyond.

Figure 1 illustrates the array of partners that might help build preparedness for such emergencies. DOE, BPS entities, and the broader electricity subsector comprise the core of the team needed to design, issue, and implement emergency orders. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>47</sup> This definition comprises the key subsector components represented in the ESCC, to include owners and operators of electric generation, transmission, and distribution assets “from all ownership categories.”<sup>48</sup> As such, the ESCC is ideally suited to coordinate with

DOE in the order development process, together with NERC, the E-ISAC, and other BPS entities and trade associations.

Surrounding these core participants are additional partners that might offer valuable insights for developing orders and coordinating emergency response operations. Some of these partners (including Congress) can also help oversee the implementation of the FPA’s emergency provisions and assess requirements for further statutory changes.

Of course, the full set of potential contributors to emergency preparedness is broader still. For example, vendors who can help utilities replace damaged relays and other equipment could play vital roles. So could law enforcement agencies, cybersecurity contractors, state National Guard organizations, and other sources of expertise and support for power companies. National laboratories and other research and development organizations will also need to sustain their support for improved grid resilience. Over time, comprehensive engagement with all such partners could pay major dividends.

<sup>47</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>48</sup> In addition to infrastructure owners and operators, ESCC membership includes regional transmission organizations and independent system operators, NERC, the National Infrastructure Advisory Council, and the Canadian Electricity Association. ESCC, *Electricity Sub-Sector Coordinating Council Charter*, 3.

## Goals and Specific Design Requirements for Developing Emergency Orders

The starting point in developing template emergency orders is to identify the objectives, scope, and design requirements that these orders will need to encompass. Key issues analyzed in the sections of the report that follow:

- **Threats, triggers, and thresholds for issuing emergency orders.** Only a limited number of natural and man-made hazards can trigger a grid security emergency.<sup>49</sup> Countering each of those hazards will require threat-specific emergency orders. Hence, the first step for developing such orders will be to examine the threats and attack scenarios on which the design process should focus and clarify the criteria that the president might use to determine that a grid security emergency exists—including when there is an “imminent danger” of an attack.
- **Designing emergency orders for sequential phases of grid security emergencies.** Different types of emergency orders will be needed to protect grid reliability (1) when attacks are imminent, and (2) when attacks are under way. Promising opportunities also exist to develop orders for a third phase of grid security emergency operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.
- **Incorporating national security policies and priorities into emergency order design.** Adversaries may strike the grid to disrupt the flow of power to defense installations and other facilities essential to national security. Many utilities are already collaborating with defense partners to build redundant power feeds for these facilities and make other targeted

investments in resilience. A growing number of grid owners and operators also plan to prioritize the restoration of power to military bases if blackouts occur. Emergency orders provide a unique opportunity for DOE and its partners to build on such initiatives, and provide more systematic, comprehensive, and effective support to national security.

An initial step to do so is to ensure that emergency orders reflect and help achieve broader federal government strategies to defend critical infrastructure. Most important, the US *National Security Strategy* specifies how the United States will deter attacks on critical systems and—if deterrence fails—how it will defeat the attackers.<sup>50</sup> DOE and its industry partners should design emergency orders to help implement the strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this design process with two further steps. First, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. The FPA provisions and existing industry plans to prioritize the restoration of power will provide a useful starting point. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement emergency orders and help defend the nation.

Emergency orders and implementation plans also offer a basis to clarify how US agencies and private companies will coordinate their operations during cyberwarfare, and build consensus on the private sector’s emerging role in national security. No power company has ever tried to maximize shareholder value by promising to bolster cyber deterrence or help defeat attacks by nations such as Russia or China. Yet, because

---

<sup>49</sup> In addition to being triggered by cyber attacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, (a)(7).

---

<sup>50</sup> White House, *National Security Strategy*, 13.



of the grid's importance to the economy, public health and safety, and national defense, the United States needs a doctrinal framework to coordinate industry and government actions during attacks on the US electric system.<sup>51</sup> Scott Aaronson, Edison Electric Institute's vice president for security and preparedness, notes that "there is not a lot of doctrine around cyber attacks on civilian infrastructure."<sup>52</sup> Building such doctrine and operationalizing public-private partnerships will be crucial for grid security emergency preparedness.

- **Communications.** The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The grid security emergency rule describes the consultative process that (if practicable) will occur before the secretary issues emergency orders.<sup>53</sup> However, the grid security emergency rule does not address the risk that adversaries will attack the industry-government communications systems necessary to issue orders, monitor their implementation, and defeat adversaries' attacks.

Building secure, survivable communications will be essential to effectively issuing and implementing emergency orders. However, the FPA provides no requirements or funding to do so. The electricity subsector is currently working with government agencies and telecommunications companies to advance secure communications initiatives. These partners should treat preparedness for grid security emergencies as a special area of focus, including measures to

ensure that grid owners and operators can verify the authenticity of emergency orders.

Government and utility leaders will also need to coordinate what they tell the American people when the secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including those for prioritized load shedding, could cut off electricity to many thousands of customers. Emergency orders that will have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Attackers will strike the grid to achieve political benefits, including, potentially, the incitement of public panic and a loss of confidence in US leaders. To promote unity of messaging against such efforts, it will be essential to build on existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders.

- **Waivers and cost recovery.** Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the act itself, FERC-approved reliability standards, or environmental regulations.<sup>54</sup> However, emergency orders will be easier to implement if they include preplanned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

<sup>51</sup> For DOD's definition of doctrine and an analysis of its benefits for joint warfighting, see Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United State*.

<sup>52</sup> Lynch, "How the Russian Government Allegedly Attacks."

<sup>53</sup> DOE, "RIN 1901-AB40," 1181.

<sup>54</sup> These waivers apply unless companies carry out orders and related actions in a "grossly negligent manner." See 16 U.S.C. § 824o-1, (f)(4).

The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.<sup>55</sup> Industry–government dialogue will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader preplanning needed for the financial turbulence that grid security emergencies could create. This study also examines possible emergency orders that would require investments in grid infrastructure to implement. The FPA does not authorize government spending on such pre-emergency projects. If DOE and its partners decide that investment-dependent orders have sufficient value for grid resilience, these partners (and Congress) should explore government funding options that reflect the national security benefits of such orders, rather than increase the electricity bills paid by private citizens.

- **Opportunities for broader resilience against grid security emergencies.** Power companies and DOE may find it helpful to develop a comprehensive plan to sequence and integrate all of the initiatives outlined above. Such a plan might also account for three additional opportunities for progress: (1) employing additional government authorities to coordinate emergency operations between electric utilities and companies in other infrastructure sectors, including the natural gas providers on which power generation increasingly depends; (2) deepening US partnerships with Canada to help protect the interconnected North American power grid, and exploring opportunities for collaboration with Mexico and other nations; and (3) examining longer-term opportunities to leverage improvements in grid resilience to strengthen cyber deterrence, and assessing the risks and potential benefits of coordinating cyber defense operations at home and abroad.

## Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies

The FPA leaves the president substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should build consensus on the types of threats that ought to drive and sequence the development process. These partners should also examine possible decision criteria and consultative mechanisms to support declarations of grid security emergencies.

### Threats That Can Trigger Grid Security Emergencies: Implications for Emergency Order Design

A broad array of natural and man-made hazards, including earthquakes and severe weather events such as hurricanes and ice storms, can cause multistate blackouts. However, in amending the FPA, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the “occurrence or imminent danger” of:

(A)

(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;<sup>56</sup> and

(ii) disruption of the operation of such devices or networks, with significant adverse

<sup>55</sup> 16 U.S.C. § 824o–1, (b)(6).

<sup>56</sup> The second section of this report defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of grid security emergency thresholds.

effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event;

or

(B)

(i) a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and

(ii) significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.<sup>57</sup>

Protecting critical and defense critical electric infrastructure against each of these threats will require different types of emergency orders—though some potential orders may be useful against multiple hazards. The threats will also pose disparate challenges for determining whether a grid security emergency is imminent or under way. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the president faces uncertainties about the likelihood and potential consequences of a grid security emergency.

### Geomagnetic Storms as a Possible Initial Focus

Emergency orders for geomagnetic disturbances will entail fewer design challenges than those for cyber attacks and other man-made hazards, and therefore provide opportunities for rapid progress. Geomagnetic disturbance events occur when coronal mass ejections on the sun create geomagnetically induced currents on the earth's surface. These currents can damage unprotected transformers and other grid infrastructure. Compared with the other threats that can trigger grid security emergencies, determining that there is imminent danger of a geomagnetic disturbance event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the president decide whether

to declare a grid security emergency and will provide significant warning before geomagnetically induced currents threaten to damage grid infrastructure.

Industry and government partners can develop emergency orders to take advantage of this warning time. For example, the secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of geomagnetically induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.<sup>58</sup>

A strong foundation already exists for drafting such orders. Studies of the effects of geomagnetic disturbances on the power grid have contributed to a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.<sup>59</sup> Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the federal government to ensure that it has the capability to predict and detect space weather events and the ability to communicate these assessments to public and private sector stakeholders. The order also requires the development of protection and mitigation plans for critical infrastructure and plans for response and recovery if geomagnetic disturbances occur. In addition, the order requires sector-specific agencies to “assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event.”<sup>60</sup>

NERC reliability standards provide an additional cornerstone for developing emergency orders for geomagnetic disturbances. TPL-007-1—*Transmission System Planned Performance for Geomagnetic*

<sup>58</sup> Phillips, “Solar Shield.” See also MISO, *Geomagnetic Disturbance Operations Plan*, 5.

<sup>59</sup> See “NOAA Space Weather Scales,” NOAA; and Kappenman, *Geomagnetic Storms*.

<sup>60</sup> Obama, *Executive Order—Coordinating Efforts*.

<sup>57</sup> 16 U.S.C. § 824o–1, (a)(7).

*Disturbance Events* establishes long-lead geomagnetic disturbance planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat for geomagnetic disturbance events.<sup>61</sup> EOP-010-1—*Geomagnetic Disturbance Operations* also requires reliability coordinators to develop geomagnetic disturbance mitigation plans and operating procedures, including specific actions that transmission operators must take based on predetermined geomagnetic disturbance-related conditions.<sup>62</sup>

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyber attacks and other man-made triggers for grid security emergencies. The sun will not intentionally hide preparations for a geomagnetic disturbance event or “prepare the battlefield” by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data that utility personnel need to maintain situational awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of critical and defense critical electric infrastructure.

The relative ease of drafting orders for geomagnetic disturbances makes such efforts a prime starting point for industry–government collaboration. The North American Transmission Forum, in coordination with the ESCC, is already examining opportunities to develop template emergency orders for geomagnetic disturbance events. But the greater degree of difficulty associated with protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of emergency orders to counter such threats. Instead,

DOE and its industry partners should consider pursuing a multitrack development process: at the same time that they seek rapid progress on emergency orders for geomagnetic disturbances, they should *immediately* accelerate the long-lead work that will be required to counter each of the man-made threats that can trigger grid security emergencies.

### Cyber and Physical Attacks

This report focuses on supporting the development of emergency orders to protect and restore grid reliability against cyber and physical attacks. In doing so, the report follows the lead of the premier electric industry exercise of grid resilience, GridEx. As in previous versions of this exercise series, GridEx IV (conducted in November 2017) employed a scenario based on large-scale, combined cyber and physical attacks against the US electric system by a highly capable adversary.<sup>63</sup> Such combined attacks could pose severe threats to nationwide grid reliability, over and above those created by cyber or physical strikes alone. Grid security emergency orders that can help power companies protect and restore reliability against combined attacks will be especially valuable for national security. Orders and implementation plans that can help counter such severe threats will also be useful in lesser contingencies, including cyber-only strikes.

Current US policy priorities focus on the need to strengthen cyber resilience for the power grid and other critical infrastructure. The US *National Security Strategy* warns that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>64</sup> DOE and its partner utilities should prioritize the development of emergency

<sup>61</sup> NERC, *TPL-007-1*.

<sup>62</sup> The standard, however, does not explicitly lay out what those predetermined conditions should be. See NERC, *EOP-010-1*. For an example of geomagnetic disturbance plans, see PJM, *PJM Manual* 13, 69–71.

<sup>63</sup> GridEx includes participation by over one hundred power companies and other components of the electricity subsector. See NERC, *Grid Security Exercise GridEx IV*, vii.

<sup>64</sup> White House, *National Security Strategy*, 12, 27.



orders to counter such attacks, and supplement the mandatory and increasingly stringent cyber critical infrastructure protection standards, as well as voluntary measures that go above and beyond those NERC requirements.<sup>65</sup>

However, orders can also help build resilience against physical attacks on the grid. Since the coordinated attack on the Metcalf substation near San Jose, California, in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high-powered rifles or other weapons. This includes NERC's *CIP-014-2—Physical Security* standard, which outlines the requirements for protecting grid infrastructure from physical attacks.<sup>66</sup> Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide-area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

An adversary would face greater risks when launching physical attacks than cyber attacks. Blowing up transformers and killing workers who are transporting replacement equipment might rapidly escalate conflict with the United States into larger-scale kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries would hide on utility networks, arming and prepositioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages that last far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk-reward calculus in our favor. If orders can help power companies protect their systems from impending physical attacks, especially in partnership with state and local law enforcement agencies, state National Guard personnel, and other sources of assistance, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Adversaries may also simultaneously employ both cyber and physical attacks. Such combined attacks can synergistically disrupt the grid in ways that cyber or physical attacks on their own cannot. For example, as in the response to cyber attacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.<sup>67</sup> However, physical attacks that destroy critical substation components or target utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

The GridEx IV scenario highlighted the unique challenges posed by combined attacks and opportunities to address them. That scenario also assumed that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging that are far more difficult to counter than in any past US power outage.

This report adopts a similarly severe threat for analyzing possible emergency orders. In particular, the report examines how orders can protect or restore grid reliability against the combined use of cyber weapons, physical attacks, and information

---

<sup>65</sup> NERC has mandatory standards for critical infrastructure protection against cyber threats. See "United States Mandatory Standards," NERC.

<sup>66</sup> DOE, *Quadrennial Energy Review*, 4–34; and NERC, *CIP-014-2*.

---

<sup>67</sup> E-ISAC and SANS-ICS, *Analysis of Cyber Attack*, v.

warfare against critical and defense critical electric infrastructure. Of course, separate types of emergency orders will be required for physical and cyber threats. Orders to deploy specific countermeasures against unmanned aerial vehicle attacks on substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead, utilities can also benefit from examining how emergency orders could help them defeat combined attacks, and how they can integrate both cyber and physical defense operations.

The study does not examine options for developing emergency orders against electromagnetic pulse (EMP) attacks. EMP threats pose a significant potential risk to the grid, and a growing (though still relatively small) number of utilities are hardening their critical systems against EMP effects.<sup>68</sup> DOE's EMP strategy provides a valuable framework and approach for managing the risks that EMP threats pose to the grid and other energy systems.<sup>69</sup> DHS's EMP strategy does the same for a broad range of infrastructure sectors.<sup>70</sup> Industry partners such as the Electric Power Research Institute are also making notable contributions to the shared understanding of EMP effects on the grid.<sup>71</sup> However, significant

research is still required to understand the combined effects of EMP wave components on grid hardware and system-wide operations and for cost-effective mitigation options and preparedness planning.<sup>72</sup> As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

## Thresholds for Declaring Grid Security Emergencies<sup>73</sup>

The FPA authorizes the president to declare a grid security emergency when there is "imminent danger" of an attack or when attacks are already occurring. However, the FPA does not further define imminent, nor provide any criteria to help determine whether the anticipated likelihood of an attack is sufficient to warrant an emergency declaration. As will be discussed below, the FPA provides guidance on the potential severity of imminent or ongoing attacks that would constitute a grid security emergency. However, those guidelines are broad and could be subject to starkly different interpretations in future crises.

Some degree of ambiguity is useful. Preserving wide presidential latitude for declaring grid security emergencies will be essential to deal with unforeseen challenges and to avoid locking US crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicize explicit red lines that would trigger a declaration. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay US defensive measures, including the issuance of emergency orders to safeguard the grid. Adversaries might even seek to spoof the president into declaring a grid security emergency when they had no intention of launching an attack—especially if adversaries believed doing so might prompt the issuance of disruptive emergency orders, crash utility stock

---

<sup>68</sup> In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to geomagnetic disturbances. The early-time component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See EPRI, *Electromagnetic Pulse and Intentional EMI Threats*, 3-3–3-4.

<sup>69</sup> DOE set strategic goals for addressing EMP threats and created an action plan to meet those goals. DOE, *Electromagnetic Pulse Resilience Action Plan*. The fiscal year 2017 National Defense Authorization Act directed DHS to create a similar strategy, which is currently in draft form. See National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328. The EPRI continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse*.

<sup>70</sup> DHS, *Strategy for Protecting and Preparing*.

<sup>71</sup> EPRI, *Electromagnetic Pulse and Intentional EMI Threats*.

<sup>72</sup> INL, *Strategies, Protections, and Mitigations*.

<sup>73</sup> The analysis in this section builds on the findings of Stockton, "Thresholds."

prices, or incite public panic in ways that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events that emergency orders should be designed to help counter.<sup>74</sup> Federal officials could also find it useful to have decision criteria to help frame their own internal deliberations and recommendations to the president. In an intense crisis, ambiguities in the FPA could fuel disagreements among the president's advisors as to whether the threat of attack was sufficiently severe to declare a grid security emergency. Developing a decision framework to support the declaration process could facilitate consensus-building and provide a structured way to integrate data on attack indicators. However, in adopting such a framework, it would also be prudent to avoid revealing any specific declaration triggers or thresholds for adversaries to exploit in their attack planning.

The section that follows examines two factors that a decision framework might encompass: the likelihood of an attack occurring and its potential consequences. This section also examines how improved information sharing between government agencies and power companies can support these assessments and recommends industry–government consultations in the declaration process that go beyond the existing provisions of the FPA.

### **Determining When Attacks Are Imminent: Criteria for Declaring Grid Security Emergencies**

In key respects, the BPS is under cyber attack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant advanced persistent threats on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS networks, secrete malware

designed to disrupt grid operations, and conduct other malicious activities to prepare for possible attacks on critical system components.<sup>75</sup> PJM Interconnection's former CEO Terry Boston recently stated that the company experiences three thousand to four thousand hacking attempts *every month*.<sup>76</sup> Penetration efforts on a similarly massive scale are likely occurring against BPS entities across the United States. While many of these efforts target information technology systems not directly involved in operating the grid, malware implants on operational technology systems are increasingly frequent and sophisticated.<sup>77</sup> And, as in the case of BlackEnergy and other campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.<sup>78</sup> The net result, according to US director of national intelligence Dan Coats: "Today, the digital infrastructure that serves this country is literally under attack."<sup>79</sup>

Of course, there is a huge gulf between implanting destructive malware on the grid and using that malware to create blackouts. The Trump administration has promised to impose "swift and costly consequences" on foreign governments and other actors who undertake "significant malicious cyber activities" against US critical infrastructure.<sup>80</sup> Attacks that create massive power outages and jeopardize US national security would be especially likely to provoke such a response. However, the president does not need to wait for blackouts to occur before declaring

<sup>75</sup> "Alert (TA18-074A)"; "Alert (TA17-293A)"; Defense Science Board, *Task Force on Cyber Deterrence*, 4; and ICF International, *Electric Grid Security and Resilience*, 19.

<sup>76</sup> Dougherty, "Biggest U.S. Power Grid Operator Suffers Attacks."

<sup>77</sup> "Alert (TA17-293A)"; and "Alert (TA18-074A)."

<sup>78</sup> BlackEnergy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of BlackEnergy inflicted the 2016 blackout on Ukraine. "Alert (ICS-ALERT-14-281-01E)."

<sup>79</sup> Barnes, "Warning Lights."

<sup>80</sup> White House, *National Security Strategy*, 13.

<sup>74</sup> Paradise et al., "ISO-RTO Council Comments," 2.

a grid security emergency. The “imminent danger” of attack is sufficient to declare an emergency and for the secretary to issue orders to help utilities ramp up their defenses.

Implants of new, potentially devastating malware across the electric grid could help the president make such a determination, particularly if other warning indicators suggest that cyber attacks are becoming increasingly likely. The geopolitical context in which cyber attacks might occur provides one such indicator. It is (barely) conceivable that adversaries will launch a “bolt from the blue” attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region and attack the grid to disrupt the deployment of US forces to the region or to achieve other military and political goals.<sup>81</sup> Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause multistate blackouts, should carry greater weight in a crisis environment.

Policy makers should consider developing a framework to assess whether these cyber preparations help justify the declaration of a grid security emergency. The US Office of the Director of National Intelligence (ODNI) has issued a cyber threat framework that could support such development efforts. The ODNI notes that government agencies, academia, and the private sector are using over a dozen analytic models to categorize cyber threats and identify changes in the activities of cyber adversaries. ODNI’s framework is intended to provide a common basis for characterizing threat activity to support analysis and senior-level decision-making.<sup>82</sup> Figure 2 illustrates the cyber threat framework.

<sup>81</sup> The section on preattack grid security emergency declarations examines these national security-related issues and their implications for designing emergency orders.

<sup>82</sup> “Cyber Threat Framework,” ODNI; and ODNI, *Common Threat Framework*, 5.

The initial stage of adversary activity is to prepare for conducting malicious activity. Adversaries then engage and establish presence on targeted systems, allowing them to “operate at will.” In the final stages, attackers seek to destroy grid hardware, software, and/or data, and prepare to conduct follow-on operations as needed to magnify the extent and duration of their disruptive effects.<sup>83</sup>

If adversaries were to suddenly make new moves into the penultimate phase (operate at will) during an intense political crisis or regional confrontation, evidence that they had done so could help the president determine whether attacks were imminent. Other independent sources of data could provide additional context for assessing adversary moves toward more threatening preattack stages. James Miller, former undersecretary of defense for policy, notes that “the United States devotes massive resources to human and technical intelligence collection of our potential adversaries.”<sup>84</sup> Such indicators could contribute to overall assessments of attack imminence.

Policy makers might also supplement the cyber threat framework with specialized attack models for the industrial control systems and other grid components that are crucial for electric system operations. The Industrial Control System Cyber Kill Chain provides an especially promising opportunity to do so. The kill chain identifies the specific sequenced phases that adversaries execute to conduct attacks that inflict predictable physical effects on grid equipment and operations.<sup>85</sup> Stage 1 begins with planning and reconnaissance against

<sup>83</sup> ODNI, *Common Threat Framework*, 13, 16.

<sup>84</sup> Miller, “Cyber Deterrence.”

<sup>85</sup> The Industrial Control System Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin in 2011 to “help the decision-making process for better detecting and responding to adversary intrusions.” The Industrial Control System Cyber Kill Chain tailors that decision-making tool for industrial control system-specific cyber threats and consequences. See Assante and Lee, *Industrial Control System Cyber Kill Chain*.



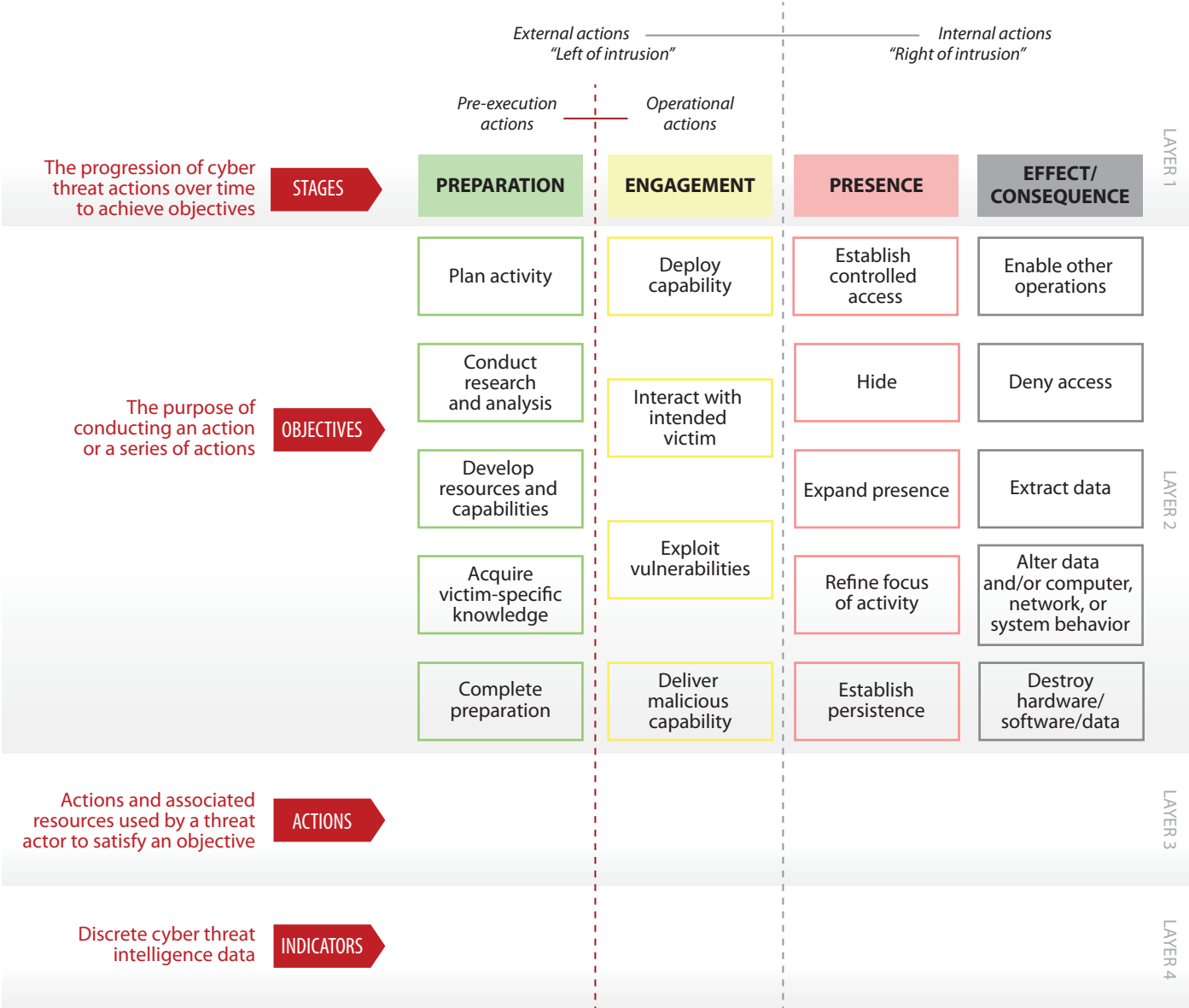


Figure 2. ODNI Cyber Threat Framework

industrial control system networks and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing attack capabilities, and—ultimately—executing the attack. Evidence of an adversary’s position along this kill chain could help support decision-making on the imminence of potential attacks, with the final phases posing the most proximate indications that an adversary is poised to strike the grid.

Potential Attack Consequences

The imminence of an attack provides only one possible criterion for declaring a grid security emergency. A second would be the potential consequences of the attack. Indeed, when Congress defined grid security emergencies in the FPA, legislators established at least implicit, consequence-based thresholds for declaring an emergency. The FPA defines grid security emergencies as occurring when attacks that are imminent or under way “could disrupt the

	General Definition	Observed Action	Intended Consequence
Level 5: Emergency (Black)	<i>Poses on imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons</i>	Effect	Cause physical consequence
Level 4: Severe (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties</i>	Presence	Damage computer and networking hardware
Level 3: High (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>	Engagement	Corrupt or destroy data  Deny availability to a key system or service
Level 2: Medium (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Steal sensitive information
Level 1: Low (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Commit a financial crime
Level 0: Baseline (White)	Unsubstantiated or inconsequential event	Preparation	Nuisance denial of service or defacement

Figure 3. Elements of the Cyber Incident Severity Schema

operation” of devices or networks that are “essential to the reliability of critical electric infrastructure or defense critical electric infrastructure.”<sup>86</sup>

However, the FPA does not clarify the extent of disruption that should trigger the declaration of an emergency. Some grid resilience stakeholders have expressed concern that policy makers might set the threshold too low, and declare grid security emergencies for minor incidents. For example, the ISO/RTO Council proposes that the use of emergency orders in such an emergency “should be reserved for true widespread emergencies.”<sup>87</sup> But

neither Congress nor DOE have yet specified what higher-level thresholds might be appropriate.

One approach to account for the potential consequences of an attack would be to leverage existing federal criteria for categorizing cyber events by the severity of their effects. The definition of “significant cyber incidents” in Presidential Policy Directive 41, *United States Cyber Incident Coordination*, provides a starting point to do so. Under the directive, significant cyber incidents are those that are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or

<sup>86</sup> 16 U.S.C. § 824o–1, (a)(7).

<sup>87</sup> Paradise et al., “ISO-RTO Council Comments,” 2.

public health and safety of the American people.”<sup>88</sup> Policy makers could apply this demonstrable-harm standard to support decisions on whether to declare a grid security emergency. If officials determine that a cyber attack is likely to inflict such harm, their finding would provide a compelling justification for making an emergency declaration.

The December 2016 *National Cyber Incident Response Plan*’s cyber incident severity schema offers a still more detailed basis to assess attack consequences. The schema (Figure 3) serves as “a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments” and agencies.<sup>89</sup> Policy makers could use the schema to help develop consequence-based criteria for declaring grid security emergencies. For example, if assessments suggest that an attack is likely to create a “level 5 emergency,” which poses “an imminent threat to the provision of wide-scale critical infrastructure services, national [government] stability, or to the lives of U.S. persons,” the declaration of a grid security emergency should be near-automatic. Level 4 events would also be very strong candidates for justifying such declarations. However, as with all such criteria, the president should also retain the latitude to make declarations for less severe incidents (for example, the disruption of a cluster of major defense installations).

One advantage of leveraging these government-wide standards is that doing so can help integrate decisions on grid security emergencies into the broader US system for incident response. As officials update the *National Cyber Incident Response Plan* and its supporting severity schema, valuable opportunities will emerge to ensure that grid security emergency declarations and operations are part of a broader, multisector approach to strengthening infrastructure preparedness.

### **Grid-Specific Criteria for Assessing Attack Consequences: Building on Standards for Adequate Levels of Reliability**

If policy makers rely only on general, government-wide decision criteria, they will miss opportunities to take advantage of the electric industry’s standards for assessing the severity of threats to grid reliability. NERC has carefully defined what constitutes adequate reliability for the power grid, as well as the types of large-scale reliability failures that owners and operators need to prevent. If utilities and government agencies have the data and analytic tools necessary to determine whether adversaries’ attacks will create such failures, their assessments could provide valuable input into decisions on declaring grid security emergencies.

The 2003 Northeast blackout spurred NERC’s efforts to define adequate levels of grid reliability and specify the types of system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over wide areas of the United States and Canada, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The 2005 amendments required FERC to certify an electric reliability organization, which will have “the ability to develop and enforce . . . reliability standards that provide for an adequate level of reliability of the bulk-power system.”<sup>90</sup> However, the FPA never defined *adequate level of reliability*; that task was left to the electric reliability organization.

When NERC became the electric reliability organization in 2006, defining the adequate level of reliability was one of its first initiatives. NERC’s board of trustees approved an initial definition for the “characteristics of a system with an adequate level of reliability” in 2008, which was updated in 2013.<sup>91</sup> Three components of NERC’s definition—cascading failures, uncontrolled separation, and instability—are

<sup>88</sup> Obama, *United States Cyber Incident Coordination*.

<sup>89</sup> DHS, *National Cyber Incident Response Plan*, 29–30.

<sup>90</sup> 16 U.S.C. § 824o, (c)(1).

<sup>91</sup> NERC, *Technical Report*, 17.

especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS.<sup>92</sup>

The sections that follow examine these three components, the reliability failures they can entail, and implications for declaring grid security emergencies. Subsequent portions of the report analyze options to develop emergency orders tailored to prevent such failures. However, in grid security emergencies, risks of all three types of failures might emerge in rapid succession and would be inextricably linked.

**Cascading failures.** NERC defines cascading as “the uncontrolled successive loss of system elements triggered by an incident at any location.” Such cascading “results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.”<sup>93</sup> NERC’s definition states that a system is adequately reliable if the system will not experience cascading failures when struck by lightning or affected by other frequent, predictable incidents (i.e., “predefined Disturbances”). But more severe events have caused instabilities that led to cascading in the past and may do so again—especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout illustrates the speed with which failures can cascade. That blackout, which affected approximately fifty million people across the United States and Canada, started with a relatively minor incident. On a hot day in August, multiple 345-kilovolt transmission lines tripped after sagging into overgrown trees. With proper situational awareness, operators might have been able to take actions to handle such a contingency, but failures in

the utility’s control room alarm processor resulted in operators being entirely unaware of the problem. In an unfortunate coincidence, the utility’s reliability coordinator also had computer problems and lacked the visual tools necessary to support grid operators.<sup>94</sup> These failures shifted power flows to a system of 138-kilovolt lines, which were unable to handle the added current flows, and overloaded the last remaining 345-kilovolt path into the area, beginning the major, uncontrollable cascading sequence.<sup>95</sup> This sequence tripped over five hundred generating units and four hundred transmission lines in only eight minutes—with most of these failures occurring *in the last twelve seconds* of the cascade.<sup>96</sup>

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversarial attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying critical generation and transmission nodes; alter protective relay settings so that grid components trip offline (or fail to do so) in ways that intensify the outages; deny grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and take other measures designed to produce cascading failures.<sup>97</sup> Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe—particularly by denying or corrupting situational awareness data.

The imminent danger or occurrence of adversary-induced cascading outages could be a criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt

<sup>92</sup> See section 215 of the FPA, which defines *reliable operation* as “operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” 16 U.S.C. § 824o, (a)(4).

<sup>93</sup> NERC, “Informational Filing,” 1, 7.

<sup>94</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>95</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>96</sup> NERC Steering Group, *Technical Analysis of Blackout*, 109.

<sup>97</sup> Cherepanov and Lipovsky, “Industroyer”; Sistrunk, “ICS Cross-Industry Learning”; “Alert (TA17-163A)”; and Dragos, *CRASHOVERRIDE*, 24.

the operation of grid devices and networks essential to critical and defense critical electric infrastructure—on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

**Uncontrolled separation.** NERC defines uncontrolled separation as “the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss.”<sup>98</sup> Severe events “resulting in the removal of two or more BES elements with high potential to cascade” can produce uncontrolled separation.<sup>99</sup>

Uncontrolled separation almost always occurs in conjunction with cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands that “quickly became unstable after the massive transient swings and system separation” because there was insufficient generation within the islands to meet electricity demand.<sup>100</sup> Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.<sup>101</sup> In the 1982 West Coast blackout, loss of 500-kilovolt lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, dividing the system into four unplanned islands.<sup>102</sup> A similar blackout in the same region in 1996, triggered by multiple major transmission line outages, again separated the Western Interconnection into four electrical islands

“with significant loss of load and generation.”<sup>103</sup> The onset of adversary-induced uncontrolled separation would provide a clear-cut basis for declaring the existence of a grid security emergency, if cascading failures had not already prompted the president to make such a determination.

**Instability.** NERC defines system instability as “the inability of the Transmission system to remain in synchronism . . . characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES.”<sup>104</sup> The BES can experience frequency, voltage, or angular instability—though none should occur during normal operating conditions.<sup>105</sup>

Severe natural hazards and other disturbances can create temporary instabilities. Grid protection systems and operational protocols typically mitigate their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, the transmission system may experience large power swings if BPS generators accelerate or decelerate too much during a disturbance, causing transmission lines to trip and generators to go out of step and trip offline, and resulting in further acceleration and deceleration—or both.<sup>106</sup> Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread cascading failures. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur. Corrupting or disabling protection systems could also make critical grid components vulnerable to physical damage from enemy-induced power surges.

<sup>98</sup> NERC, “Informational Filing,” 6.

<sup>99</sup> NERC, “Informational Filing,” 13.

<sup>100</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 75.

<sup>101</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 104.

<sup>102</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 105.

<sup>103</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 106.

<sup>104</sup> NERC, “Informational Filing,” 6.

<sup>105</sup> NERC, “Informational Filing,” 1–2.

<sup>106</sup> NERC, “Informational Filing,” 6.



Evidence that adversaries were taking preparatory measures to create widespread instabilities could help the president determine that a grid security emergency exists.

However, it may be difficult to predict whether an impending attack will create such failures. The first requirement to do so will be to determine the extent to which adversaries have embedded advanced persistent threats or established other means of attack across the grid—a task that adversaries will complicate by attempting to hide their malware from detection. The next step will be to rapidly characterize these threats, assess the vulnerability of utility systems to them, and predict the consequences for grid reliability if the enemy strikes. Such assessments will also need to account for system-wide effects involving the interaction of multiple adversary-induced disruptions, which may compound and reinforce instabilities in ways that are difficult to predict. PJM Interconnection, LLC, the regional transmission operator for much of the Mid-Atlantic and some neighboring states, recently noted that “additional study is needed to better understand the expected impacts of a large-scale cyber-attack.”<sup>107</sup> Given these challenges, it may be difficult to fully predict the potential impact of cyber attacks on grid reliability until attacks are well under way.

But it could also be risky to wait until attacks are occurring to declare a grid security emergency. In the 2003 Northeast event, for example, cascading blackouts spread across vast areas in seconds. If the president delays declaring a grid security emergency until cascades are under way, emergency orders designed to help prevent their spread may come too late. A better option might be to make an early decision based on imperfect assessments, especially if (as this report recommends) DOE can issue preattack emergency orders that will bolster grid defenses without disrupting normal electric service.

In particular, the president could consider declaring a grid security emergency if (1) an attack appears to be increasingly likely, and (2) assessments indicate that the impending attack may create cascading blackouts or other widespread instabilities. Figure 4 illustrates one option for developing a decision support framework that accounts for the likelihood and potential consequences of an attack. The vertical axis depicts the ODNI cyber threat framework’s four stages of adversary actions, from potential attack preparations to actual strikes against the grid. An adversary’s sudden, large-scale moves up this axis—especially in the context of a severe international crisis—could help the president determine that an attack is impending. The horizontal axis represents the risk that if an attack occurs, the grid will experience cascading failures and other widespread instabilities that would inflict demonstrable harm to national security, the economy, or public health and safety. Attacks that pose little or no risk of cascading blackouts might not warrant the declaration of a grid security emergency.

However, systemic threats to grid reliability are far from the only consequence-based criteria that the president might want to consider. More narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security, such as the National Capital Region, might be sufficient to declare a grid security emergency. Policy makers could develop more refined decision frameworks to account for a broad array of consequence thresholds, as well as further criteria for assessing attack imminence.

## Data Sharing and Consultations with Industry

The electric industry can provide data and analytic support to help the president and other officials decide whether to declare a grid security emergency. Power companies will have direct access to the malware that adversaries implant on their networks, and will be well positioned to assess the potential

---

<sup>107</sup> PJM, “Comments and Responses,” 35.

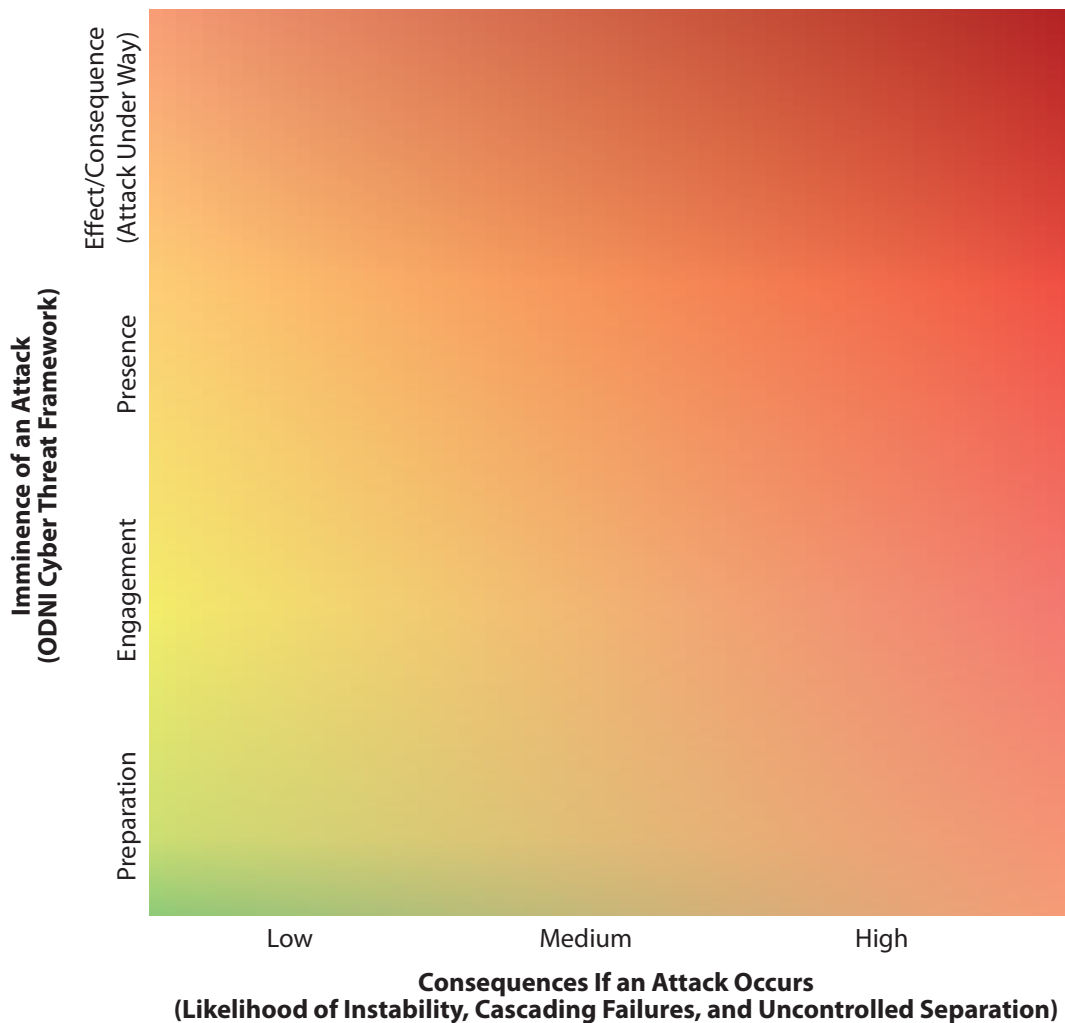


Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies

impact of various attack vectors on their systems and on the grid as a whole.

Government agencies and cyber contractors can help utilities target searches for this malware and provide additional value for the declaration process. If a regional crisis or other geopolitical factors increase the risk of cyber attacks on the grid, agencies should be prepared to ramp up information sharing with BPS entities, especially in terms of specific signatures or other threat indicators to search for in utility networks, logs, and critical equipment.

Industry and government should also explore how ongoing threat detection and analysis initiatives could directly help assess the imminence and

potential consequences of attacks. For example, DOE has projects under way to bolster situational awareness for operational technology networks that could be applied to support such assessments. The department is developing capabilities to monitor traffic on operational technology networks via the Cybersecurity for the Operational Technology Environment project.<sup>108</sup> Other department-funded projects could prove useful for the emergency declaration process as well.<sup>109</sup>

<sup>108</sup> DOE, *Multiyear Plan*, 23.

<sup>109</sup> See, for example, the Containerized Application Security for Industrial Control Systems, Survivable Industrial Control Systems, and Research Exploring Malware in Energy Delivery Systems projects. “Sandia’s Grid Modernization Program

Utilities and DOE might also refine ongoing information sharing initiatives to directly support the emergency declaration process. For example, DOE's Cybersecurity Risk Information Sharing Program is a public-private partnership to build bidirectional situational awareness and facilitate classified and unclassified information sharing.<sup>110</sup> DOE's 2018 cybersecurity plan launched additional activities to advance industry participation in the program, as well as its analytic tools and capabilities.<sup>111</sup> The program is managed by NERC and the E-ISAC, which play an integral role in sharing information and establishing situational awareness within the electricity subsector.<sup>112</sup> In addition, FERC recently issued a proposed directive for NERC to expand reporting requirements for cyber incidents, including for those that "might facilitate subsequent efforts to harm the reliable operation of the bulk electric system."<sup>113</sup> All of these efforts could be integrated to support assessments of the likelihood and potential consequences of attacks.

DHS's May 2018 cybersecurity strategy provides a broader approach to expand information sharing. Most important, the strategy could enable data from other infrastructure sectors to support the declaration process, especially from communications systems and other sectors that support power restoration operations. The strategy also calls for the expansion of automated mechanisms to receive, analyze, and share cyber threat indicators, defensive measures, and other cybersecurity information with critical infrastructure and other key stakeholders.<sup>114</sup>

Such automated sharing mechanisms will be vital to accelerate the identification and assessment of malware that could pose imminent threats to grid reliability. DHS's Automated Indicator Sharing capability "enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed."<sup>115</sup> This bidirectional information sharing will limit an adversary's ability to compromise multiple systems with the same malicious code. The Defense Advanced Research Projects Agency is also working on new technologies to protect the grid. In particular, the agency's Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is working with companies to develop prototype capabilities for improving attack detection, response, and forensics support.<sup>116</sup> Moreover, as automated malware detection and analytic techniques improve, utilities may be able to speed their evaluation of potential intrusions and slash the number of false positives that current detection systems generate.<sup>117</sup> All of these initiatives should be leveraged to help the president determine whether to declare a grid security emergency.

Policy makers should also consider preplanning to consult with grid owners and operators in the declaration process. The FPA leaves the president with sole authority to declare a grid security emergency. If a potential emergency surfaced, the president would almost certainly draw on the expertise and recommendations of the secretary of energy, as well as other members of the National Security Council and supporting agencies. But power companies and their industry organizations will also have perspectives on operational and technical issues that could prove valuable for assessing potential attacks.

---

Newsletter," Sandia National Laboratories; and "REMEDIYS," Cyber Resilient Energy Delivery Consortium.

<sup>110</sup> "Energy Sector Cybersecurity Preparedness," DOE.

<sup>111</sup> DOE, *Multiyear Plan*, 23.

<sup>112</sup> "Electricity Information Sharing and Analysis Center," NERC.

<sup>113</sup> FERC, *Cyber Security Incident Reporting Reliability Standards* (161 FERC ¶ 61,291), 2.

<sup>114</sup> DHS, *Cybersecurity Strategy*, 13.

---

<sup>115</sup> "Automated Indicator Sharing (AIS)," US-CERT.

<sup>116</sup> Douris, "DARPA Research."

<sup>117</sup> Ucci, Aniello, and Baldoni, "Survey on Machine Learning," 1:5; McElwee et al., "Deep Learning"; and McElwee, "Probabilistic Cluster."



Neither the FPA nor the grid security emergency rule explicitly provide for consultations with industry on whether to declare a grid security emergency. The FPA calls for consultations “to the extent practicable” before the secretary issues emergency orders.<sup>118</sup> But there are no equivalent provisions to include industry input in the emergency declaration process.

Industry and government partners should explore options to provide for such consultations, preferably by leveraging existing mechanisms under the ESCC and E-ISAC. As with consultations on issuing orders, urgent circumstances could shorten or preclude opportunities for government dialogue with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of “bolt from the blue” attacks. Nevertheless, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be invaluable for determining whether (and when) to declare a grid security emergency.

## Grid Security Emergency Phases and Order Design Options

DOE and its industry partners should consider designing emergency orders for three potential phases of grid security emergencies. First, if the president determines that there is an imminent danger of an attack, the secretary should be ready to issue preattack orders that help utilities protect grid reliability. Second, once attacks are under way, the secretary could issue orders to reduce the risk of cascading failures or other widespread disruptions of electric service. Third, as utilities begin to restore grid reliability, orders could help utilities replace damaged equipment and counter adversary efforts to disrupt restoration operations.

Orders for each phase of a grid security emergency will differ not only in terms of when the secretary would issue them but also in the degree to which they

will disrupt normal electric service. Some orders, such as staffing up emergency operations centers before an attack occurs, would leave customers unaffected. In contrast, orders for prioritized load shedding could temporarily halt service to many customers—but could also greatly reduce the risk that instabilities will lead to cascading blackouts.

Figure 5 provides examples of orders that vary in the degree of disruption they would inflict on normal service, and also in the way they would meet the phase-specific challenges of grid security emergencies. The analysis that follows examines each of them (and other possible orders) in greater detail.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, emergency orders for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are under way. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies “stop the bleeding” from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are under way.<sup>119</sup> Adversaries may also launch follow-on attacks once utilities begin focusing on restoration. Emergency orders to help utilities repel such attacks could become essential components of the restoration process.

<sup>118</sup> 16 U.S.C. § 824o–1, (b)(3).

<sup>119</sup> In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is fully restored to pre-event conditions) as the “new normal”—characterized by “degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months.” See Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

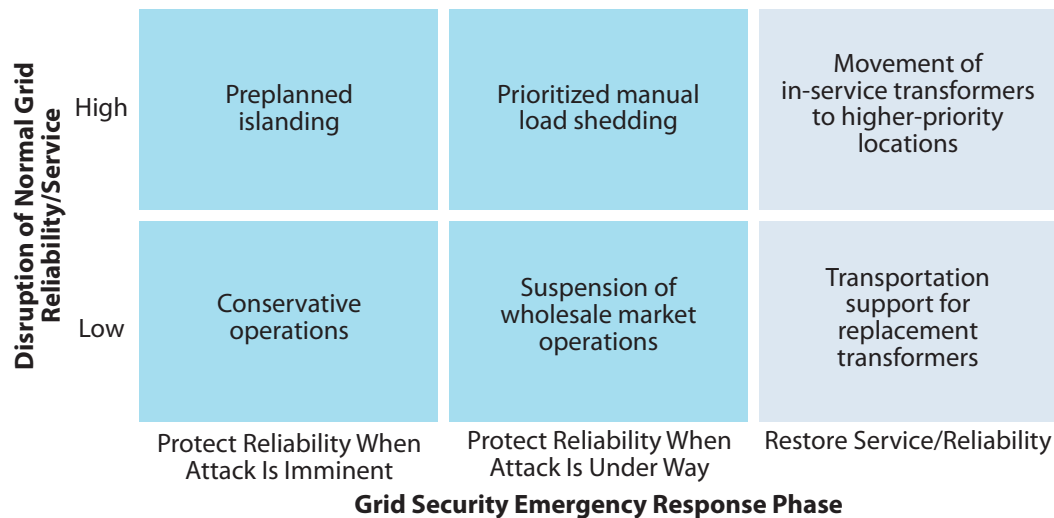


Figure 5. Emergency Order Matrix: Examples of Order Designs

DOE and its partners will need flexibility to deal with the overlapping phases of grid security emergencies. Nevertheless, being able to categorize potential orders in terms of when they would likely be issued and which phases of emergency operations they could support can help establish a systematic process for developing orders.

Creating emergency orders for all three phases can also help utilities and DOE integrate the orders into seamless, multiphase operational plans for grid security emergencies. As intense regional crises or other events elevate the risk of attacks on the grid, it will be prudent to preplan for the issuance of emergency orders for multiple grid security emergency phases. Orders for preattack measures such as conservative operations would be issued first if attacks are deemed imminent. At the same time, however, DOE and the utilities subject to emergency orders should be using any available warning time to prepare for the issuance and implementation of orders for the midattack and restoration phases.

## Preattack Options

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal

with these ambiguities is to delay the declaration of a grid security emergency until blackouts begin; doing so would forego the benefits of issuing preattack emergency orders. It may be possible to develop orders that will offer significant benefits if adversaries strike yet also have little or no impact on normal service—thereby offering “no-regrets” options to employ when the likelihood of an attack remains uncertain. Industry and government partners should also explore options for the preattack phase that would be more disruptive but also offer potentially far-reaching benefits. These two options occupy the left-hand column in Figure 5.

Conservative operations that utilities employ against natural hazards provide a model for protecting the grid in ambiguous preattack situations. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects and prepare for possible response and restoration operations if grid infrastructure is damaged.<sup>120</sup> For

<sup>120</sup> Conservative operations are not defined in the NERC glossary of terms. However, many reliability coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken to “implement

example, reliability coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.<sup>121</sup> Power companies may also cancel noncritical generation and transmission maintenance activities; reduce transfer limits to give the transmission system extra “slack”; and staff their backup control centers, critical BPS substations, and other vital facilities to set the stage for emergency operations as hurricanes approach.<sup>122</sup>

A defining feature of these frequently used conservative operations is that they do not disrupt normal service to customers. Their negligible service impact makes them more viable to implement when the storm’s path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the US coast. Instead, they provide a wide “cone of uncertainty” that becomes increasingly narrow as the hurricane approaches. Utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other conservative operations. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these operations do not affect normal service to customers enhances the willingness of utility leaders to order their implementation while the storm track remains uncertain.

---

additional actions to ensure the BES remains reliable in the face of the additional threats” when “events, conditions, or circumstances may put the Bulk Electric System (BES) at an increased level of risk, compared to normal operating conditions.” See PJM, “Conservative Operations,” 3. Similarly, the Western Electricity Coordinating Council, defines conservative systems operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets “are restricted and managed in order to maintain or restore reliability of the power system from the negative influence of a triggering event or condition.” See Western Electricity Coordinating Council, “Conservative System Operations,” 4.

<sup>121</sup> PJM, “Conservative Operations,” 3.

<sup>122</sup> PJM, “Conservative Operations,” 9.

Industry and government partners should borrow from this model to develop orders for preattack conservative operations against cyber and/or physical attacks. Some have already begun to do so. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting conservative operations to meet the specialized challenges posed by cyber and physical threats.<sup>123</sup> This preparation will be extremely helpful as potential attacks loom. As a regional confrontation or other precipitating crisis intensifies, it is conceivable that the US intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. However, it is much more likely that ambiguities will persist about whether the adversary will actually attack and risk a devastating US response. To ensure that sufficient time is available to implement conservative operations, the secretary may need to order the initiation of such measures when enemy intentions remain uncertain—and when warning indicators may turn out to be false.

Many of the conservative operations that will bolster resilience against adversary attacks would be similar to those developed for natural hazards. For example, preattack emergency orders might direct BPS entities to increase generation reserves and/or re-dispatch resources out of least-cost operations. Other orders might be threat specific: for example, to intensify scrutiny of operational technology networks for malware and implement government-vetted counter-measures in ways that give utilities sufficient latitude to account for their unique system characteristics.

The common denominator for all such options: if the secretary issues orders for BPS entities to adopt conservative operations and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented the orders.

---

<sup>123</sup> See, for example, PJM, *PJM Manual* 13, 73; Lucas, “Conservative Operations”; and SERC, *Conservative Operations Guidelines*.

However, because so many utilities already have robust plans and capabilities to protect their systems from imminent threats, close government–industry coordination will be required to ensure that emergency orders actually assist grid defense rather than function as speed bumps or useless distractions. Reliability coordinators and other grid operators serve as the pointy end of the spear for protecting grid reliability. Mandatory NERC standards require BPS entities to maintain voltage stability, automatic load shedding schemes, and contingency reserves for disturbances.<sup>124</sup> NERC standards also require transmission operators to “develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area.”<sup>125</sup> Balancing authorities have similar requirements to manage generating and demand-side resources in their service areas.<sup>126</sup> These plans are exercised, tested, and frequently updated to bolster their effectiveness for actual emergencies. While many of NERC’s mandatory standards apply when disturbances begin to occur, BPS entities are spring-loaded to implement conservative operations the moment potential hazards begin to emerge.

If major grid disruptions occur, BPS entities will not sit on their hands and wait for the president to declare a grid security emergency and the secretary to issue emergency orders. Indeed, DOE does not contemplate that they will. In the final grid security emergency rule, the department states that the declaration of a grid security emergency “does not preclude electric utilities from taking time-sensitive action to secure the safety, security, or reliability of the electric grid prior to the issuance of an emergency order.”<sup>127</sup>

DOE and its partners can design emergency orders to help supplement and support such industry-led operations. For example, government agencies may acquire highly classified indicators that an attack is imminent. Declaring a grid security emergency and issuing emergency orders for conservative operations could ensure that utilities bolster their preparedness against such attacks on a consistent, nationwide basis, including those utilities that had not yet identified a need to act. Orders to help power companies ramp up and target searches for specific types of malware could supplement utilities’ defensive operations as well. The secretary might also issue orders to ensure that such industry operations benefited from the FPA’s regulatory protections and cost-recovery provisions.

### More Disruptive Preattack Options

Many utilities are also prepared to take pre-event emergency measures that will significantly disrupt normal electric service, yet also offer benefits far beyond those that conservative operations can provide. For example, power companies can selectively halt electric service on warning of catastrophic storm surges. If seawater hits systems that are still carrying electricity, transformers and other difficult-to-replace grid components will suffer catastrophic physical damage. In 2012, weather forecasters warned that Superstorm Sandy might produce storm surges that would inundate critical substations and underground electrical equipment in lower Manhattan. Consolidated Edison’s team made the politically difficult decision to prevent such damage by preemptively cutting of power to the area. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.<sup>128</sup> Moreover, Consolidated Edison limited the shutdown’s disruptiveness by notifying customers hours earlier that the utility might halt service and by already having plans in place to prioritize the

<sup>124</sup> See, for example, NERC, *VAR-001-4.2*; NERC, *Standard PRC-006-3*; NERC, *PRC-010-2*; and NERC, *BAL-002-2(i)*.

<sup>125</sup> NERC, *EOP-011-1*, R1.

<sup>126</sup> NERC, *EOP-011-1*, R2.

<sup>127</sup> DOE, “RIN 1901–AB40,” 1177.

<sup>128</sup> Miller, “Con Edison Shuts off Power.”



restoration of service to hospitals, water-pumping stations, and other critical facilities.<sup>129</sup>

BPS entities continue to use “shutdown on warning” as an effective tool to avoid equipment damage against severe weather and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent equipment damage and speed up restoration. Generation owners similarly chose to shut down or evacuate some generating units in the storm’s projected path.<sup>130</sup>

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and heating and air conditioning systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

DOE and its electricity subsector partners should consider developing emergency orders that offer a similar set of risks and rewards. However, doing so will entail problems beyond those associated with protecting the grid against natural hazards. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an adversary will actually pull the (cyber) trigger and whether attacks are likely to cause demonstrable harm to the US economy, national security, or public health and safety. Measures developed for natural hazards may also offer uncertain benefits against imminent cyber and physical attacks. For example, further analysis will be required to determine whether and how preattack grid shutdowns might help counter specific cyber threats, including attacks that disable

protection systems to facilitate equipment-damaging power surges.

Other disruptive emergency orders could counter a broader range of threats but entail major (and perhaps insurmountable) problems for nationwide employment. The upper left-hand box in Figure 5 offers a prime example of such options: preplanned power islanding. Microgrids offer the most familiar means of establishing power islands.<sup>131</sup> A growing number of military bases, universities, and major hospitals have sufficient generation and other electric infrastructure on-site so that if adversaries black out the surrounding grid (or pose an imminent danger of doing so), those facilities can separate from the grid and operate independently as power islands.

However, microgrids do not offer “bulletproof” power resilience. Cyber adversaries are sure to treat on-base electric infrastructure, including renewable generation assets, as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas-fired generators, the power they provide is only as resilient as the gas transmission and distribution systems that supply them—and cyber threats to natural gas systems are rapidly escalating.<sup>132</sup> Moreover, building microgrids requires extensive investment in grid infrastructure. Investment demands will be especially heavy if installations want to serve not only the critical loads within their perimeters but also the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to building microgrids, power companies are also analyzing ways to establish emergency power islands with less infrastructure investment. One particular option being explored by GridEx participants is to preplan to establish large

<sup>129</sup> DiSavino and Sheppard, “ConEd Cuts Power.”

<sup>130</sup> NERC, *Hurricane Harvey*, v.

<sup>131</sup> DOE’s definition of microgrids: “A microgrid is a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously.” “The Role of Microgrids,” DOE.

<sup>132</sup> DOE, *Quadrennial Energy Review*, 7-7; and Parfomak, *Pipelines*, 2-3.



power islands by using existing grid infrastructure within their boundaries. Utility personnel have noted that they might be able to use legacy balancing areas as a starting point to establish island boundaries. On warning of an imminent attack or under other extraordinary circumstances, utilities would separate a power island from the surrounding grid and operate independently to serve critical loads within it. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, preplanned islands might become a hedge against cascading failures and uncontrolled separation.

In practice, preplanned islanding will be practical only if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for preplanned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands to enable them to function independently of the grid. Moreover, standing up islands would severely disrupt day-to-day service for noncritical customers and create instabilities for surrounding systems that could produce additional service disruptions. Accordingly, preplanned islanding might be considered a “huge-regrets” emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created.

DOE and its industry partners should also consider developing preattack emergency orders that fall between the two extremes of no-regrets options and highly disruptive measures. For example, to avoid remote execution of destructive malware on utility networks, orders might direct utilities to disconnect their systems from the internet. Utilities could also take additional measures to isolate or compartmentalize all control systems. Implementing these

measures would curtail potential attack vectors, but would do so at a price. Disconnecting from the internet would hobble wholesale market operations, disable email as a basic communications tool, affect an entity’s access to other means of communications (i.e., E-ISAC and DOE portals), impact an entity’s ability to comply with regulatory requirements, and produce other undesirable consequences. Any unexpected challenges in isolating or compartmentalizing the control systems that are critical to the functioning of the grid could also jeopardize normal service. Nevertheless, if industry and its government partners can preplan to anticipate and overcome these challenges, even highly disruptive preattack options may be useful to protect the grid from cascading failures.

## Extraordinary Measures when Attacks Are Occurring

Emergency orders when attacks are underway can help utilities prevent widespread instabilities, cascading failures, and uncontrolled separation. Under the auspices of the ESCC, utilities and their resilience partners are already developing “extraordinary measures” to operate the grid if adversaries disable or corrupt SCADA (supervisory control and data acquisition) systems, state estimators, and other operational technology hardware and software components on which utilities typically rely.<sup>133</sup> For example, the North American Transmission Forum is leading an initiative on supplemental operating strategies to help power companies manually cope with the loss of energy management systems and/or SCADA across a large geographic footprint.<sup>134</sup>

---

<sup>133</sup> These extraordinary measures include resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary backup systems, and development of supplemental operating strategies use in “degraded states.” See “ESCC: Electricity Subsector Coordinating Council,” ESCC.

<sup>134</sup> Galloway, “Advancing Reliability and Resilience of the Grid,” 2.

These industry efforts provide a basis to develop grid security emergency orders for extraordinary measures when attacks are under way. So, too, do existing BPS emergency operating plans, capabilities, and operational requirements to manage the grid instabilities. Options for such orders vary in terms of the disruption they would inflict on normal grid operations.

Figure 5 provides an example of a low-disruption order for this phase: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate needs or for the next day). These entities have taken extensive measures to keep market functions separate from their operational control of the grid. Many entities also have mechanisms in place to operate when markets are temporarily suspended. Over extended periods, however, cyber attacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, undercut the valuation of power companies on Wall Street, and magnify the damage to the US economy that attacks on the grid will create.

Regional transmission organizations are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the transmission operator<sup>135</sup> for the Mid-Atlantic and other US regions, has called for the development of mechanisms to permit “nonmarket” operations in extreme circumstances.<sup>136</sup> A number of options exist to provide for such operations. For example, if the secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell

power at a fixed price predetermined by DOE.<sup>137</sup> Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high-benefit/low-disruption emergency orders, including orders for maximum power generation when attacks are under way, will also fall into this category.<sup>138</sup>

Industry and government partners will also need to develop more disruptive emergency orders that can protect grid reliability in extraordinary circumstances. One option to do so involves operating an area in a generation-deficient state for a prolonged period, supported (when practical) by power imported from neighboring regions. The top center box of Figure 5 provides another prominent example: prioritized manual load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by selectively shedding load and implementing rotating blackouts.<sup>139</sup>

A failure to shed load contributed to the cascading failures in the major 2003 blackout. After-action reports from that event found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission

<sup>135</sup> The NERC glossary defines *transmission operator* as “the entity responsible for the reliability of its ‘local’ transmission system, and that operates or directs the operations of the transmission facilities.” *Transmission operator area* is defined as “the collection of Transmission assets over which the Transmission Operator is responsible for operating.” See NERC, *Glossary*.

<sup>136</sup> PJM, “Comments and Responses,” 6, 39–40.

<sup>137</sup> Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. PJM, “Comments and Responses,” 39.

<sup>138</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual* 13, 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see MISO, “MISO January 17–18 Maximum Generation Event Overview.”

<sup>139</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 11.

lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. A US–Canada task force found that “timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio.”<sup>140</sup> In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.<sup>141</sup>

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for transmission operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation for building emergency orders to reduce the risk that physical and cyber attacks will create cascading blackouts.

One way to shed load would be to order power companies to execute rotating blackouts. In such controlled outages, grid operators interrupt service on a rotating basis to sequential sets of distribution feeders for limited periods (typically twenty to thirty minutes).<sup>142</sup> Grid operators employed rotating blackouts to help protect grid reliability during the “Big Chill” that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT’s rotating blackouts during the event affected a total of 4.4 million customers.<sup>143</sup> The temporary blackouts were no doubt disruptive. However, by reducing the risk of cascading failures, those

outages offered compelling system-wide benefits for protecting reliability.

But rotating blackouts will not offer the best option for load shedding in all grid security emergencies. In the event of a massively disruptive attack, an emergency order might require utilities to shed load without implementing rotating blackouts, because such rotating outages could introduce unacceptable reliability risks during a chaotic and rapidly changing situation. As an alternative, utilities can implement “brownouts”: that is, conduct voltage reductions to maintain a continual balance between supply and demand within a balancing area.<sup>144</sup> However, brownouts and rotating blackouts share a serious limitation: they affect all customers equally. But not all customers will be equally important in a grid security emergency. DOE and industry will need orders and implementation plans for manual, prioritized load shedding, so utilities can focus on sustaining power flows to hospitals and other critical loads while also reducing the risk of cascading power failures. NERC already requires BPS entities to have plans for both automatic and manual load shedding.<sup>145</sup> Utilities and DOE should use these requirements as the starting point to design emergency orders for extraordinary measures that would supplement what BPS entities are already prepared to do to if major instabilities occur.

## Emergency Orders to Support Power Restoration

The rightmost column in Figure 5 provides the third category for emergency orders: those that can help grid owners and operators restore power after widespread

<sup>140</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 147.

<sup>141</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 77.

<sup>142</sup> NERC, *Reliability Terminology*, 1.

<sup>143</sup> FERC and NERC, *Restoration and Recovery Plans*, 61.

<sup>144</sup> NERC, *Reliability Terminology*.

<sup>145</sup> NERC standards currently emphasize automatic load shedding to protect grid reliability. See NERC, *Standard PRC-006-3*; and NERC, *PRC-010-2*. However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing emergency orders to prevent or mitigate cascading failures. See NERC, *EOP-011-1*.

outages occur. In past cascading failures of the US electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days (and in some cases much less time) because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators, transmission lines, and other system components are designed to trip offline when instabilities occur, thereby protecting them from damaging power surges—and leaving them available to help rapidly reestablish the flow of power.<sup>146</sup> However, if cyber or physical attacks destroy critical system components, requirements to repair or replace such assets could greatly lengthen and complicate the restoration of service. Emergency orders can support restoration operations and better align them with national-level priorities.

Emergency orders for the restoration phase can also account for the risk that adversaries may continue their attacks as power companies begin to restore service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to US military bases and other vital facilities and to seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeting power restoration operations can help adversaries achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply. Risks of reattack should help drive the design of restoration-phase emergency orders.

Advanced persistent threats hidden in utility networks will pose especially significant challenges for restoration. This malware may enable adversaries to conduct recurring attacks based on timing or network

conditions. Unless utilities thoroughly eradicate such malware, repeated outages could impede restoration operations and put the grid at sustained risk of cascading failures.<sup>147</sup> Physical attacks against restoration personnel and replacement equipment in transit would pose additional problems. Grid security emergency orders can help utilities restore electric service even if they remain “under fire” from cyber and kinetic weapons.

Such orders will differ in the degree to which they could alter existing utility plans to restore power. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks, and barges) from where power companies store them to where they are needed as replacements.<sup>148</sup> Subsequent portions of this report examine how DOE could collaborate with other federal agencies and state and local officials to waive transportation regulations and bolster security support for such operations. The secretary could also issue orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, ports, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these prioritized customers. Emergency orders can help incorporate other national security-related assets that utility plans do not typically include, such as components of the defense industrial base essential for resupplying US forces abroad.

DOE and its industry partners should also create template emergency orders for in extremis restoration operations that would more sharply depart from existing industry plans and procedures. The upper right-hand box of Figure 5 offers an example

<sup>146</sup> NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, 1.

<sup>147</sup> Homeland Security Advisory Council, *Final Report*, 7.

<sup>148</sup> DOE, *Strategic Transformer Reserve*, 12–13.



of one such option. If adversaries damage or destroy an extraordinarily large number of transformers, the secretary might order utilities to remove surviving in-service transformers in the same voltage class from their substation and transport them to serve vital national security facilities in the National Capital Region or other areas. Orders of this kind could create severe disruptions in existing service. They might even impede system restoration if utilities and their government partners have not adequately prepared to account for challenges regarding transformers' technical specifications and the BPS's overall configuration. However, if these challenges can be addressed, the benefits might be greater still for helping the United States defeat its adversaries.

Other in extremis orders could help utilities operate the grid if equipment damage is so extensive (or reattacks are so effective) that full system restoration will require many weeks or even months. The FERC/NERC study on severe impact resilience (May 2012) found that coordinated cyber and physical attacks may force the grid into a "new normal" state of "degraded planning and operating conditions" that could last for months or years, including reduced generation and transmission resources and planned and unplanned rotating blackouts.<sup>149</sup> DOE and power companies should consider how emergency orders and supporting regulatory waivers might help electric utilities serve priority loads and accelerate restoration under new normal conditions.

One option to do so is to preplan for the waiver of selected reliability standards. The *Severe Impact Resilience* study recognized that catastrophic events could "put entities in a position where they cannot comply with all standards." However, in part due to the difficulty of predicting the circumstances that entities will face, the study recommended against preplanning for waivers. Instead, the study proposed relying on entities to "do the right thing" for reliability

and public safety" and self-report violations as circumstances permit.<sup>150</sup>

NERC should reconsider this conclusion in light of the secretary's new grid security emergency authorities and the waiver provisions they entail. FERC, NERC, and their industry and government partners should identify specific regulatory waivers and related measures that could provide the basis for utilities' contingency planning for new normal operations.

One such option lies in reliability standards for managing unforeseen contingencies. Currently, NERC standards require BPS entities to operate in an N-1 state: that is, they must be able to sustain service even if they suffer the most severe single contingency (such as the loss of a single critical line, transformer, or generator) possible in their system.<sup>151</sup> Operators may be required to shed load prior to any contingency to maintain the N-1 state. These requirements apply during normal day-to-day operations as well as during system restoration.

Returning to an N-1 state in the face of coordinated cyber and physical attacks is likely to be a lengthy process involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. To help enable utilities to serve critical facilities during such sustained events, the secretary might issue emergency orders that explicitly allow utilities to function in an N-0 operating state (as long as doing so did not risk causing cascading failures or equipment damage).<sup>152</sup>

Issuing such orders could entail important benefits. Operating at N-0 would give utilities greater operating flexibility and ensure that entities can continue to serve as much load as possible during a grid security

---

<sup>149</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

<sup>150</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 17.

<sup>151</sup> NERC, *BAL-002-2(i)*, requirement R2; NERC, *TOP-001-3*, R12 and R14; and NERC, *IRO-008-2*, R5 and R6.

<sup>152</sup> For N-0, all elements must be within thermal and voltage limits prior to any contingency.



emergency, including military installations and other priority customers. Unlike under N-1 operations, entities would be required to shed load only prior to any contingency for the most severe single contingencies if any of those single contingencies would cause cascading failures, or after a contingency that required load shedding to eliminate overloads or low voltage.

But operating at N-0 would also entail significant risks. N-1 standards exist for compelling reasons: they help protect grid reliability against severe contingencies. Deviating from N-1 requirements will create greater risks of causing further blackouts in new normal conditions. Moreover, N-0 operations would require even greater coordination among BPS entities (including reliability coordinators, transmission owners, and local control centers), as a single outage could result in equipment overloads or voltage violations and require extraordinary mitigation measures. Accordingly, this option will be feasible only if DOE partners with FERC, NERC, and entities to fully understand and mitigate such risks, as well as maximize the potential benefits of N-0 operations for serving critical national security-related loads.

## Additional Emergency Order Design Parameters and Supporting Initiatives

Adversaries will attempt to black out the US grid to achieve their broader political, economic, and military objectives in a conflict. Government agencies and the electricity subsector should design emergency orders to help prevent attackers from accomplishing their objectives, and—ideally—to help deter them from attacking at all.

However, deterring and defeating attacks on the grid will require resilience improvements beyond the electricity subsector. Attackers may simultaneously strike electric and communications systems to both disrupt the grid and impede the issuance and

implementation of emergency orders. Adversaries may also seek to incite public panic through social media and other information warfare operations to advance their broader political objectives. Countering such efforts will require unprecedented collaboration among utilities, government agencies, media, and the broader telecommunications sector.

Designing and implementing emergency orders to blunt attacks by Russia, China, and other potential high-capability adversaries will place extraordinary burdens on electric utilities—burdens that few ratepayers and utility investors will be eager to bear on their own. To help power companies meet these challenges, it will be essential to fully leverage the regulatory waiver and cost-recovery provisions of the FPA, and examine whether Congress should expand these provisions as threats continue to intensify.

## Deterring and Defeating US Adversaries

The US *National Security Strategy* emphasizes that cyber threats to US critical infrastructure are becoming increasingly severe. In particular, the strategy notes that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>153</sup> Pairing cyber attacks with coordinated physical strikes against transformers and other critical grid infrastructure would exacerbate these disruptive effects.

The strategy identifies two primary means for deterring catastrophic attacks, both of which can be supported by emergency orders and implementation plans:

- (1) Convince adversaries that they will suffer “swift and costly consequences” if they strike the grid or other US targets, and that the United States “can and will defeat them” if deterrence fails.<sup>154</sup>

<sup>153</sup> White House, *National Security Strategy*, 13, 28.

<sup>154</sup> White House, *National Security Strategy*, 28.

- (2) Strengthen infrastructure resilience to create “doubt in our adversaries that they can achieve their objectives” if they do attack (i.e., deterrence by denial).<sup>155</sup>

### **Deterrence through Cost Imposition: Protecting Defense Critical Electric Infrastructure**

In amending the FPA, Congress placed a particular emphasis on the need to protect the reliability of defense critical electric infrastructure (i.e., grid components that serve military bases and other facilities “critical to the defense of the United States” and vulnerable to the disruption of grid-provided electricity).<sup>156</sup> Emergency orders to protect such infrastructure can help ensure that US bases have the power they need to respond to attackers. But prioritizing defense installations for support in grid security emergencies will require deeper analysis of US deterrence requirements, given DOD’s growing dependence on civilian assets and functions to execute defense missions. Deterrence by cost imposition will also depend on convincing potential adversaries that the United States will be able to identify them as the perpetrators of attacks on the grid. DOE and its industry partners should explore how emergency orders can facilitate attack attribution, as well as provide broader support for the credibility of the US deterrence posture.

A relatively small number of military bases are responsible for inflicting unacceptable costs on potential adversaries. The US Defense Science

Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of US strike systems (cyber, nuclear, and nonnuclear) and supporting infrastructure to ensure “that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks.”<sup>157</sup> Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which US strike systems rely and ensure that they have reliable power even in extended conflicts.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The strategy emphasizes that “we must convince adversaries that we can and will defeat them—not just punish them if they attack the United States.”<sup>158</sup> Defeating adversaries in regional contingencies in the South China Sea, the Baltics, or other potential conflict zones will place special burdens on US grid resilience. US capabilities to conduct operations abroad are increasingly dependent on domestic military and civilian assets. In particular, a vast array of US defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy, operate, and sustain US power projection forces for regional conflicts.

This dependence makes the grid a prime target for attack. The DOD *Mission Assurance Strategy* notes that adversaries may seek to disrupt power projection capabilities by attacking the domestic infrastructure systems on which they depend. In particular, the strategy warns that “potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting

<sup>155</sup> White House, *National Security Strategy*, 13, 28. The literature on security studies defines deterrence by denial in a variety of ways. This report follows the definition used in the *National Security Strategy*, which is consistent with the definition employed in the Obama administration’s deterrence policies. See Lynn, “Defending a New Domain.” For broader studies of deterrence by denial, and critiques of the way in which the strategy employs the term, see Fischerkeller and Harknett, “Deterrence Is Not a Credible Strategy”; Mitchell, “Case for Deterrence by Denial”; Gerson, “Conventional Deterrence,” 40; and Nye, “Deterrence and Dissuasion,” 56–58.

<sup>156</sup> 16 U.S.C. § 824o–1, (a)(4).

<sup>157</sup> Miller and Gosler, “Memorandum.” See also pp. 3, 6–7, 11–12, and 17–18 of the report.

<sup>158</sup> White House, *National Security Strategy*, 28.

critical defense and supporting civilian capabilities and assets,” including the US power grid.<sup>159</sup>

Ensuring the availability of resilient power for ports and other civilian assets essential for power projection will require emergency orders to serve an expanded set of customers, far beyond those responsible for strike operations. These orders will also need to encompass a much larger array of defense critical electric infrastructure owners and operators.

Electric companies and defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds from separate high-voltage transmission substations to serve defense installations provides a valuable means of strengthening resilience against physical attacks.<sup>160</sup> Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.<sup>161</sup> Utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as power islands independent of the surrounding grid.<sup>162</sup>

While valuable, these initiatives do not eliminate the need to develop national defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases and will not necessarily provide resilience against cyber attacks (since even redundant feeds may share common cyber vulnerabilities). Emergency generators will break down in long-duration outages. Moreover, resupplying them with fuel will become increasingly difficult at installations that lack massive storage

tanks. Large-scale microgrids for islanded operations can provide more resilient power. DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction and scale them to serve infrastructure loads outside the base that are essential for on-base operations. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for war fighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, including the intermodal transportation systems that help deploy and sustain US forces abroad.

DOE and its industry partners can design emergency orders to support US deterrence credibility and power projection capabilities far more quickly and with less infrastructure investment. However, for utilities to implement these orders, they must first know which customers are of the highest priority for sustaining and restoring service when enemies strike. Section 215A of the FPA provides the ideal starting point develop and share such data. The act requires the secretary of energy, in consultation with other federal agencies and grid owners and operators, to identify and designate “critical defense facilities” in the forty-eight contiguous states and the District of Columbia that are “(1) critical to the defense of the United States; and (2) vulnerable to a disruption of electric energy provided to such facility by an external provider.”<sup>163</sup> Congress’s definition of defense critical electric infrastructure also helps guide implementation of that requirement. Such assets include “any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]” as a critical defense facility, “but is not owned or operated by the owner or operator of such facility.”<sup>164</sup>

<sup>159</sup> DOD, *Mission Assurance Strategy*, 1.

<sup>160</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39.

<sup>161</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 40.

<sup>162</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39. See also Van Broekhoven et al., *Microgrid Study*; and Marqusee, Schultz, and Robyn, *Power Begins at Home*, 13–15. A number of “islandable” microgrid projects are under way at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See McGhee, “EEI Executive Advisory Committee,” 4; and Kaften, “DoD Tests Energy Continuity.”

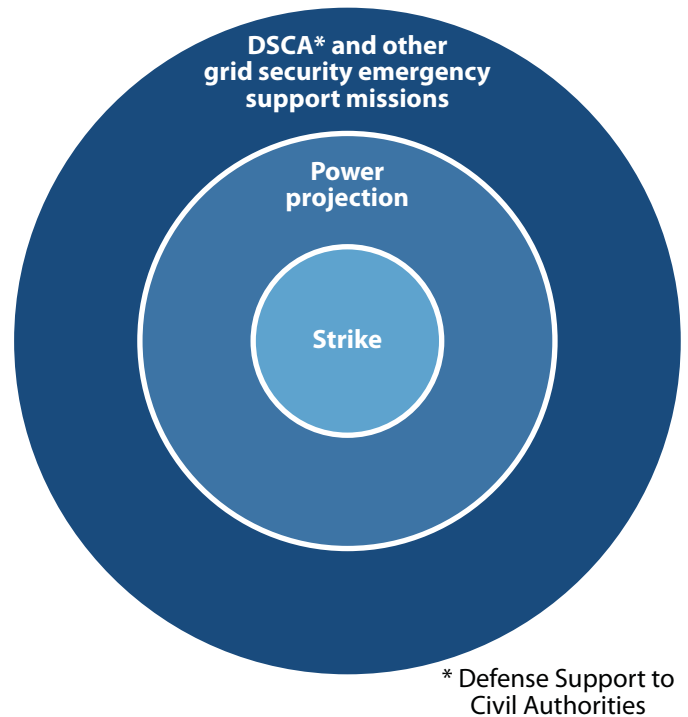
<sup>163</sup> 16 U.S.C. § 824o–1, (c).

<sup>164</sup> 16 U.S.C. § 824o–1, (a)(4).

DOE is already working with DOD to identify defense critical electric infrastructure and the installations this infrastructure serves. DOD has a well-established, continuously updated list of critical military bases and other DOD assets to support this identification process.<sup>165</sup> However, deterrence and power projection will also depend on sustaining electric service to a diverse array of ports, transportation systems, and other civilian-owned infrastructure. Figure 6 illustrates how DOE, DOD, and their partners might categorize all such defense-related assets and the defense critical electric infrastructure that grid security emergency orders should help protect.

At the innermost core lie those installations and supporting infrastructure capable of inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital. Protecting the reliability of the defense critical electric infrastructure on which they depend should be the top nationwide priority for developing emergency orders and company-specific implementation plans.

The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining these assets abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the US grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. DOD is in the process of identifying the specific facilities and supporting infrastructure that are required to help execute operational plans around the globe.<sup>166</sup> The department also has well-established criteria and assessment methods to prioritize these supporting assets for risk mitigation.<sup>167</sup> DOD and DOE should use these tools to identify the broader set of defense critical electric infrastructure needed for deterrence



**Figure 6. Categories for Protecting Defense Critical Electric Infrastructure**

and to help power companies preplan to support critical assets within their service footprints.

The third circle includes the still larger array of defense installations, including National Guard bases, which would be essential for providing defense support to civil authorities if disruptions of the grid jeopardize public health and safety.<sup>168</sup> During Hurricane Maria (2017), Superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, lodging, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and delivering other assistance. Protecting or rapidly restoring the reliability of the defense critical electric infrastructure that supports

<sup>165</sup> See DOD, *Manual 3020.45*; and DOD, *Directive 3020.40*.

<sup>166</sup> DOD, *Directive 3020.40*.

<sup>167</sup> DOD, *Manual 3020.45*.

<sup>168</sup> Of course, many National Guard installations that could conduct defense support operations may also be responsible for assisting war fighting operations abroad, and would therefore fall within the second circle as well.



these defense-support-to-civil-authorities functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public.<sup>169</sup>

Building preparedness for grid security emergencies can also help meet an underlying challenge for deterrence: attack attribution. To convince foreign leaders that they will suffer swift and costly consequences if they strike the grid, those leaders must first believe that the United States will be able to identify them as the attackers.<sup>170</sup> The Federal Bureau of Investigation (FBI) and other federal agencies are improving their attribution capabilities.<sup>171</sup> US agencies also devote massive resources to human and technical intelligence collection on potential adversaries, which could further assist attack attribution.<sup>172</sup> Nevertheless, adversaries may seek to strike in ways that complicate attack forensics by employing wiper tools and using other tactics, techniques, and procedures to cover their tracks.<sup>173</sup>

Emergency orders can help defeat adversaries' efforts to evade attribution. By refining the FPA's information sharing mechanisms and building them into emergency orders, utilities and their government partners can strengthen their ability to share malware samples and other information on threat signatures.<sup>174</sup> New technologies can bolster such collaboration. For

example, the Containerized Application Security for Industrial Control Systems project is designed to help grid operators isolate and capture malware on their systems, enabling samples to be shared with government agencies while still preventing that malware from disrupting system operations.<sup>175</sup>

Developing emergency orders and implementation plans to defend the grid can also provide broader support for attribution. James Miller notes that "while cyber hardening of US critical infrastructure will never be good enough to prevent a Russia or China from being able to threaten a major attack, it can cause them to have to be 'noisier' to do so, thereby boosting our confidence in attribution."<sup>176</sup> Emergency measures to protect grid reliability can complicate attack planning and, ideally, drive adversaries to strike in ways that will make them easier to identify.

### **Deterrence by Denial: Protecting Critical Electric Infrastructure**

Convincing adversaries that they will suffer unacceptable costs if they strike the grid is only one means of deterring such attacks. Another means is to reduce the benefits that adversaries expect to achieve by attacking. In classical deterrence theory, both factors combine to influence an adversary's decision on whether to strike. As Joseph Nye Jr. puts it, "deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."<sup>177</sup>

The *National Security Strategy* calls for measures that can prevent attackers from achieving the goals they seek and thereby strengthen deterrence by denial. The strategy states that "we must ensure the ability to deter enemies by denial, convincing them that they cannot accomplish their objectives through the use of

<sup>169</sup> Countering such adversary efforts will also require protecting electric service to financial institutions, regional hospitals, and other civilian assets essential to the US economy and public health and safety. The next section of the report examines these requirements and their implications for deterrence and emergency order design.

<sup>170</sup> On the tasks that attribution comprises, see Lin, "Escalation Dynamics," 49–50.

<sup>171</sup> Smith, "Roles and Responsibilities." See also Newman, "Hacker Lexicon."

<sup>172</sup> Miller, "Cyber Deterrence."

<sup>173</sup> Newman, "Hacker Lexicon."

<sup>174</sup> See 16 U.S.C. § 8240–1, (d). Later sections of this report provide a more detailed assessment of provisions for improved information sharing.

<sup>175</sup> "Sandia's Grid Modernization Program Newsletter," Sandia National Laboratories.

<sup>176</sup> Miller, "Cyber Deterrence."

<sup>177</sup> Nye, "Deterrence and Dissuasion," 45.



force or other forms of aggression.”<sup>178</sup> Ensuring that the grid and other infrastructure sectors can survive attacks and rapidly recover from service interruptions plays an especially important role in the administration’s deterrence posture. The strategy notes that “a stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.”<sup>179</sup> More recent statements of administration policy also note that deterrence by denial “must be foundational to the U.S. deterrence approach,” and that US efforts must continue “to deny adversaries the benefits of their malicious cyber activities.”<sup>180</sup>

Emergency orders and implementation plans may be able reduce the benefits that adversaries expect to achieve by attacking the grid. Preattack orders to bolster grid defenses can impede adversary efforts to disrupt grid reliability. Once attacks are under way, orders for prioritized load shedding and other extraordinary measures can help limit the damage the adversaries may hope to inflict on financial institutions, hospitals, and other electricity-dependent facilities. Orders that accelerate power restoration to these critical facilities may also reduce the effects of an attack, and thereby strengthen deterrence by denial.

The FPA is ready-made to support such improvements. In addition to protecting defense critical electric infrastructure, and thereby assisting deterrence through cost imposition, the act also authorizes orders to protect a much broader portion of the grid: critical electric infrastructure. Such infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>181</sup> Orders to help utilities defend critical electric infrastructure can reinforce deterrence by denial—and, if deter-

rence fails, reduce the devastation that adversaries will create.

However, developing and implementing such orders will entail major challenges. Some deterrence theorists doubt whether deterrence by denial is practical in cyberspace, in part because offensive capabilities are so much stronger than cyber defenses. The conclusion of this report will examine those arguments and explore broader opportunities to bolster deterrence and help the United States defeat our adversaries if conflicts nevertheless occur. First, however, DOE and its partners will need to overcome two impediments to protecting critical electric infrastructure: determining which specific facilities and functions are truly critical, and securely sharing that information with utilities so they can refine their operational plans for grid security emergencies.

### **Building a “Section 9+ List:” Prioritizing Infrastructure for Sustainment and Restoration**

Identifying and prioritizing critical electric infrastructure will be far more difficult than doing so for defense critical electric infrastructure. If adversaries create cascading blackouts across one or more interconnections, the disruption of many thousands of civilian-owned facilities could negatively affect national security, the US economy, and public health and safety. Utilities cannot possibly prioritize the flow of power to all such facilities. Government agencies and their private sector partners will need to determine which specific customers (and the critical electric infrastructure that serves them) are most vital to the nation and must continue to receive power if widespread instabilities occur.

Executive Order 13636 (February 2013) provides an existing methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the secretary of homeland security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security,

<sup>178</sup> White House, *National Security Strategy*, 28.

<sup>179</sup> White House, *National Security Strategy*, 13.

<sup>180</sup> DOS, *Recommendations*, 2.

<sup>181</sup> 16 U.S.C. § 824o–1, (a)(2).

or national security.”<sup>182</sup> That standard—catastrophic damage—provides a useful criterion to identify the highest-priority assets and associated critical electric infrastructure for protection by emergency orders in grid security emergencies. Over time, orders and contingency plans could gradually encompass less-critical facilities and grid infrastructure.

Of course, the section 9 methodology and subsequent list were never intended to support the implementation of section 215A of the FPA. As a result, the section 9 methodology falls short of meeting all the requirements for supporting emergency order design. One gap lies in the threats that drive the selection of critical assets. Section 9 focuses exclusively on infrastructure at risk from cyber attacks. The FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on electric systems. Executive Order 13636’s section 9 requirements also create a “corporate”-level list that is not broken down into the key assets within those corporations (i.e., facilities, systems, and nodes). More fine-grained data and analysis will be required to identify facilities for which sustained electric service will be most crucial. Efforts to prioritize grid service will also need to account for the increasingly complex interdependencies between US infrastructure sectors.<sup>183</sup>

Despite these shortfalls, Executive Order 13636’s methodology can provide a valuable starting point for identifying the most vital critical electric infrastructure and supporting assets. DOE and its industry partners should leverage that methodology to create a “section 9+” list, tailored to fulfill FPA emergency order requirements. Other government initiatives to prioritize critical infrastructure could

also make valuable contributions to the list and overall prioritization effort. For example, DHS’s May 2018 cyber strategy emphasizes the importance of “identifying the most critical [federal] systems and prioritizing protections around those systems.”<sup>184</sup> A number of other initiatives could provide significant value as well.<sup>185</sup> Building a section 9+ list would also benefit from the inclusion of input from cleared state regulators and homeland security and emergency management officials.

DHS’s National Risk Management Center can help integrate these sources of data and develop a comprehensive, cross-sector basis for prioritizing the sustainment and restoration of power to critical facilities. Government agencies within the center will collaborate with the private sector to “identify, assess, and prioritize efforts to reduce risks to national critical functions, which enable national and economic security.” One immediate task will be to “help define what is truly critical.”<sup>186</sup> As this work

<sup>184</sup> DHS, *Cybersecurity Strategy*, 8.

<sup>185</sup> There are numerous programs that DOE and its partners could leverage to build the section 9+ list. DHS’s National Critical Infrastructure Prioritization Program aims to identify “nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance.” See DHS, *NIPP 2013*, 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on “lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity” (p. 24). Despite its focus on terrorist threats, *Homeland Security Presidential Directive 7* also requires the secretary of homeland security to identify and prioritize systems and assets that, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the “loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States” and lower jurisdictions. The national-level priorities on this list could also be helpful. 6 U.S.C. § 124l, (a)(2).

<sup>186</sup> “National Risk Management Center Fact Sheet,” DHS.

<sup>182</sup> Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*.

<sup>183</sup> For methodologies and data-gathering strategies to assess cross-sector interdependencies, see EIS Council, *E-PRO Handbook III*; and Homeland Security Advisory Council, *Final Report*.

goes forward, the center's efforts could contribute to the development of a section 9+ list that will be essential for grid security emergency preparedness.

### **Sharing the Section 9+ List and Protecting Critical Electric Infrastructure Information**

In addition to identifying assets most in need of power, it will also be essential to share that data with the utilities responsible for providing prioritized service. Current section 9 guidance lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the federal government tells grid owners and operators if they are on the section 9 list, it rarely informs them about the section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own system configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data with government partners. Public sector leaders will need to reinforce their industry counterparts' confidence that government agencies will not use company-provided information for regulatory compliance, antitrust, or other purposes not explicitly approved through industry-government dialogue.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that critical companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations or supply chains in one industry can produce unintended and unforeseen effects on overall system resilience. Private

companies will need to help government agencies modify the section 9+ list as they reconfigure their operations and create new dependencies on outside service and product providers.

Securing and limiting the distribution of this classified data will also be a prerequisite for countering potential attacks. If adversaries acquired the section 9+ list, it would provide a roadmap that they could use to maximize their devastation of US critical infrastructure. However, measures to protect this data must be complemented by improved mechanisms to provide sensitive information to industry personnel who have the requisite security clearances.

Section 215A of the FPA offers a starting point to meet these requirements. The FPA provides for the sharing of critical electric infrastructure information, defined as information generated by FERC or other federal agencies related to identified (or proposed) critical electric infrastructure "that is designated as critical electric infrastructure information by the Commission or the Secretary" or that qualifies under FERC's critical energy infrastructure information scheme.<sup>187</sup> The FAST Act amendments directed FERC to facilitate the voluntary sharing of such information "with, between, and by" BPS entities and their government partners.<sup>188</sup> The amendments also require FERC to create criteria and procedures to designate certain information as critical and prohibit unauthorized disclosure of that information.<sup>189</sup> To help meet these requirements, FERC incorporated and is building on its well-established mechanisms to protect critical energy infrastructure information.<sup>190</sup>

<sup>187</sup> The definition excludes classified national security information. 16 U.S.C. § 824o-1, (a)(3).

<sup>188</sup> This includes NERC, the E-ISAC, regional entities, and "other entities determined appropriate by the Commission." See 16 U.S.C. § 824o-1, (d)(2)(D).

<sup>189</sup> 16 U.S.C. § 824o-1, (d)(2).

<sup>190</sup> FERC, *Regulations Implementing FAST Act Section 61003* (Order No. 833), 157 FERC ¶ 61,123, 13. See also FERC,

Other initiatives are also under way to provide for the protected data sharing essential for preplanning grid security emergency operations. DOE is working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate assets identified as defense critical electric infrastructure. Going forward, DOE, FERC, and their industry partners should refine their equivalent mechanisms to securely distribute data on critical electric infrastructure and the water systems, communications centers, and other essential non-defense assets that must continue to function in grid security emergencies.

## Communications Requirements for Issuing and Employing Emergency Orders

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phones and other normal means of communication fail. These systems often provide connectivity with neighboring BPS entities and, to an increasing extent, entities that are farther away. Under the ESCC, industry has also built an extensive set of playbooks to help companies decide what to tell customers about an incident and to unify messaging between government officials and industry representatives on estimated times of restoration and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. Preparedness for grid security emergencies will require additional progress in four areas: (1) refining consultative mechanisms and protocols for the sequential (though potentially overlapping) phases of such emergencies; (2) ensuring that communications

systems can survive adversaries' attacks; (3) authenticating emergency orders and protecting the security of sensitive data; and (4) determining what to say to the US public and accounting for the risk that adversaries will conduct information warfare operations to intensify panic and incite disorder.

## Initial Consultations and Sustained Communications

As with the phases of grid security emergency declarations, the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Preattack consultations constitute the initial stage. As noted above, the FPA specifies that before the secretary issues emergency orders, DOE will consult with power companies and other BPS stakeholders "to the extent practicable . . . regarding implementation of such emergency measures."<sup>191</sup> This report recommends that federal officials also consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The grid security emergency rule clarifies how DOE's Office of Electricity Delivery and Energy Reliability will consult on emergency orders.<sup>192</sup> The rule states that, if practicable, the E-ISAC is one of the organizations the secretary will consult. Such consultations will be particularly useful for sharing data (including classified data) on attacks that are imminent or under way. The rule also notes that DOE will consult with the ESCC. The ESCC will provide an especially valuable source of industry perspectives on grid security emergency declarations and emergency orders because it represents all components of the electricity subsector and has extensive experience in coordinating the industry's incident response operations. In addition, the rule states that "efforts

*Regulations Implementing FAST Act Section 61003* (Order No. 833-A), 163 FERC ¶ 61,125; and 18 CFR 388.113.

<sup>191</sup> DOE, "RIN 1901-AB40," 1774.

<sup>192</sup> DOE, "RIN 1901-AB40," 1181.



will be made” to consult with NERC, regional entities, “owners, users, or operators” of critical and defense critical electric infrastructure (including regional transmission operators), appropriate federal and state agencies, and other grid reliability stakeholders.

Issuing emergency orders constitutes the second stage. DOE’s grid security emergency rule states that the department will “communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances.”<sup>193</sup> The E-ISAC will likely play a critical role in such communications, since it maintains a detailed, continuously updated list of all BPS owners, operators, and registered users (distribution entities). DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.<sup>194</sup> As long as these mechanisms can be hardened as necessary to survive adversaries’ attacks, leveraging them for grid security emergencies will be much more efficient than creating a separate, unfamiliar system for communicating emergency orders.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders. Attacks on the grid are unlikely to be “one and done.” As adversaries continue to try to destabilize the grid, and power companies respond with emergency operations to protect and restore electric system reliability, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional orders and response activities—potentially on a nationwide basis.

Reliability coordinators will be a critical touchpoint between DOE and individual BPS entities, serving as a focal point between DOE (and other government

leaders) and the power companies that are in their purview. This positioning makes them well suited to communicate secretary-issued orders to individual utilities. Moreover, given reliability coordinators’ responsibilities and authorities to help maintain grid reliability when incidents occur, they will also be ideally positioned to understand how grid security emergency orders should supplement BPS emergency operations that are already under way.

Sustained communications will also be necessary to meet an additional FPA requirement: responding to DOE requests for information on the implementation of emergency orders. The grid security emergency rule specifies that “beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order.”<sup>195</sup> Sustained communications links between DOE and BPS entities will be required to meet such requests for information. However, beyond compliance issues, continuous communications will also be required as government and industry partners assess the effectiveness of emergency operations and identify requirements for additional actions.

### Survivability of Communications

Adversaries will have compelling incentives to combine attacks on the grid with strikes against US communications systems. The 2015 attack on Ukraine’s electric grid illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone networks; the latter attack prevented customers from reporting outages and disrupted grid operators’ ability to conduct restoration operations.<sup>196</sup> In turn, if adversaries can lengthen power outages by disrupting communications systems essential

<sup>193</sup> DOE, “RIN 1901-AB40,” 1181.

<sup>194</sup> DOE, “RIN 1901-AB40,” 1177.

<sup>195</sup> DOE, “RIN 1901-AB40,” 1182.

<sup>196</sup> “Alert (IR-ALERT-H-16-056-01).”



for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications-system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually reinforcing disruptions in both sectors.

We should assume that adversaries will design their attacks to maximize multisector failures, especially since they would already be facing the risk of US response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry–government coordination in grid security emergencies. Enemies might strike communications systems to hobble efforts to share preattack threat data and convey emergency orders. Once attacks on the grid were under way, adversaries could also seek to cripple the communications systems needed to coordinate emergency operations and assess requirements for additional measures.

Strengthening the survivability of existing communications links will be essential to manage these risks. To date, ESCC consultation and coordination mechanisms have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to distributed denial-of-service attacks and a range of other increasingly severe threats,<sup>197</sup> as well to the loss of the grid-provided electricity on which many such systems depend (especially in long-duration outages that put emergency power assets at risk).

Adversaries may also seek to disrupt systems essential for information sharing. For example, the Cybersecurity Risk Information Sharing Program and other E-ISAC notification procedures and portals are in place to alert utilities when adversaries

are implanting malware on critical systems.<sup>198</sup> This includes the E-ISAC's new Critical Broadcast Program, which is intended to operationalize the organization's information sharing capabilities.<sup>199</sup> The FBI and DHS also issue alerts to the energy sector, as in the case of CrashOverride.<sup>200</sup> However, many of these warning and information sharing mechanisms rely on the internet or other potentially vulnerable systems. Industry and government should explore options to ensure that they can still convey essential data in the face of sophisticated attacks on the communications sector.

In addition, adversaries may seek to disrupt the issuance of emergency orders. DOE's grid security emergency rule notes that the department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include "essential actions" to protect BPS reliability, which require recipients to respond as defined in the alert.<sup>201</sup> DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across registered entities. NERC already distributes alerts broadly to BPS users, owners, and operators in North America. Hence, the alert system provides DOE with an opportunity for "one-stop shopping" when issuing emergency orders. The secretary could issue an order to NERC for distribution to both regional operating organizations (regional transmission organizations, independent

<sup>197</sup> Banham, "DDoS Attacks."

<sup>198</sup> "Energy Sector Cybersecurity Preparedness," DOE; and "Electricity Information Sharing and Analysis Center," NERC.

<sup>199</sup> The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See Lawrence, de Seibert, and Daigle, "E-ISAC Update."

<sup>200</sup> "Alert (TA17-163A)."

<sup>201</sup> "About Alerts," NERC.

system operators, reliability coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is email based.<sup>202</sup> As such, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also includes only those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for implementing emergency orders for prioritized load shedding and other actions to sustain power to critical facilities.

Moreover, while the NERC alert system could provide a means of communications across BPS users, owners, and operators, NERC primarily uses the system to communicate alerts of voluntary actions to be taken by electric industry stakeholders. Using the NERC alert system to instead communicate a mandatory action pursuant to a DOE emergency order would require clear coordination and communication to ensure that the order and associated requirements for action are fully understood. In addition, while the NERC alert system offers a proven means to convey unclassified information, the system may not be well suited to distribute classified data.

To fill these gaps, industry and government partners should consider measures to bolster the NERC alert system or create fallback options for survivable communications. Satellite phones offer a prominent option for operational coordination. These phones are widely deployed both among BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies.

Retired US Air Force General William Shelton, who directed the US Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community."<sup>203</sup>

Accordingly, power companies are ramping up their investments in terrestrial emergency communications systems that are hardened against cyber and physical attacks and can be used to sustain critical grid functions even if satellite phones fail.<sup>204</sup> Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are under way to build dark fiber or other survivable links between BPS entities—much less between those entities and DOE. The National Infrastructure Advisory Council study *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish "separate, secure communications networks specifically designated for the most critical cyber networks, including 'dark fiber' networks for critical control system traffic and reserved spectrum for backup communications during emergencies."<sup>205</sup>

The council's study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. In doing so, DOE should leverage lessons learned from the communications sector and specifically from the National

<sup>202</sup> "About Alerts," NERC.

<sup>203</sup> Shelton, "Threats to Space Assets," 3.

<sup>204</sup> FERC and NERC, *PRASE*, 15.

<sup>205</sup> NIAC, *Securing Cyber Assets*, 7.

Security Telecommunications Advisory Committee, which has extensive experience in building redundant and survivable systems.<sup>206</sup> However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities “can communicate with utility crews working in the field to manually restore power” and conduct other postattack operations.<sup>207</sup> Survivable communications systems must also be able to coordinate emergency operations across the electricity subsector and with supporting government agencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when those orders are needed most.

### Authenticating and Securing Emergency Orders

In addition to disrupting the availability of communications systems, adversaries may also seek to corrupt the content of emergency orders and coordination messages, and gain access to classified US data to help defeat grid protection measures. One near-term requirement will be to ensure that utilities can authenticate the orders they receive from DOE. Power companies will need to be able to verify that an order has actually come from the secretary, and that adversaries have not altered its content. Verifying the authenticity of orders will be especially important if such orders require extraordinary measures that could further disrupt normal service and affect public health and safety.

Existing mechanisms and protocols to ensure the integrity of subsector communications provide an initial basis to meet these challenges. Other government agencies have also developed authentication protocols that could be adapted for use in grid security emergencies. For example, the *DoD Cybersecurity Discipline Implementation Plan* (February 2016) offers detailed guidance to strengthen authentication in the face of adversary

efforts to exploit communications networks and devices.<sup>208</sup>

Adversaries may also seek to gain access to classified or operationally sensitive emergency orders. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as possible, lest those operations create incentives for adversaries to strike before their advanced persistent threats were disabled. When attacks are under way, it could be useful to deny adversaries the knowledge of where and how BPS entities are prioritizing the flow of power to vital military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important, given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The FPA and subsequent grid security emergency rule provide for the sharing of classified information in grid security emergencies. The rule specifies that:

To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.<sup>209</sup>

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program already have mechanisms and protocols for sharing and securing classified threat

<sup>206</sup> “About NSTAC,” DHS.

<sup>207</sup> NIAC, *Securing Cyber Assets*, 7.

<sup>208</sup> DOD, *DoD Cybersecurity Discipline Implementation Plan*.

<sup>209</sup> DOE, “RIN 1901–AB40,” 1182.

data with BPS entities cleared for access to that data.<sup>210</sup> Industry and government partners should consider building on those mechanisms to support the issuance of classified emergency orders. Ongoing progress under the Cybersecurity Risk Information Sharing Program will be valuable as it serves a growing array of utilities, accesses additional sources of data and advanced analytic tools, and continues other improvements.

DOE and its partners in industry and government might consider sharing this classified data in other ways. For example, DHS and other federal partners such as the FBI and the National Guard have secure video teleconference capabilities. However, these are technologically complex and not seamlessly interoperable with industry systems. Moreover, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Section 215A addresses this issue by ordering the secretary to “facilitate and, to the extent practicable, expedite,” the security clearance process for key personnel of any entity subject to emergency orders to enable “optimum communication” of threat information.<sup>211</sup> DOE should accelerate its ongoing efforts to meet this requirement. The section also grants the secretary and other appropriate federal agencies the authority to provide temporary access to classified information regarding grid security emergencies and subsequent orders to key personnel of complying entities.<sup>212</sup>

Yet, even for utilities with cleared personnel on their staffs, an even smaller number possess the sensitive compartmented information facilities or other infrastructure and government approvals to store classified information. To address those limitations, the grid security emergency rule clarifies that the secretary may declassify information critical to the

emergency response.<sup>213</sup> But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of combatant commander operational plans; when emergency orders may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

### Communicating with the American People

Adversaries may attack the grid not only to disrupt national defense and the economy but also to gain political leverage over US leaders by inciting public panic and disorder. A presidential declaration that the grid faces imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the US public.

Preplanning for public messaging to accompany grid security emergency declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Unifying messaging with governors and other elected officials on estimated restoration times already presents significant challenges in such events. However, those difficulties will be dwarfed by the problems that adversaries can create through cyber attacks. Attackers may:

- Use information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety
- Intensify state and local requests for defense support to civil authorities to deal with these

<sup>210</sup> “Energy Sector Cybersecurity Preparedness,” DOE.

<sup>211</sup> 16 U.S.C. § 824o–1, (e).

<sup>212</sup> 16 U.S.C. § 824o–1, (b)(7).

<sup>213</sup> DOE, “RIN 1901–AB40,” 1778.



anticipated effects, and thereby put pressure on US leaders to divert scarce defense assets and resources from other missions

- Disrupt normal means of communication on which the public will rely for information about the event
- Magnify the inherent difficulties of estimating restoration times by employing advanced persistent threats that enable repeated reattacks and disruptions in grid service until eradicated from BPS networks.

DHS's Social Media Working Group for Emergency Services and Disaster Management has offered preliminary recommendations on how to counter disinformation during disaster response operations.<sup>214</sup> In addition, the ESCC and its members are developing playbooks to help meet disinformation challenges and support public messaging in the event of cyber or physical attacks against the grid.<sup>215</sup> Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that presidential grid security emergency declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Preplanning for message coordination with Canada and Mexico could also be helpful and might leverage the FPA's provisions for such multinational consultations concerning the issuance of emergency orders.<sup>216</sup>

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. For example, some orders that will be valuable for protecting grid reliability, including those for prioritized load shedding, could

cut off electricity to many thousands of customers to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

## The Deeper Value Proposition for Emergency Orders: Political Top Cover, Waivers, and Cost Recovery

The grid security emergency provisions of the FPA do not even mention a significant advantage that orders can provide for industry: they can help protect power companies from the political heat that extraordinary grid protection measures will create. The FPA's provisions for regulatory waivers and cost recovery offer more explicit benefits. Yet, given the risks that utilities could incur in conducting emergency operations, and the investments in infrastructure that may be required to facilitate order implementation, Congress and DOE should consider additional measures to help power companies defend the grid and protect national security.

### Facilitating Operations under Extraordinary Political Circumstances

In responding to natural hazards, power companies can fall under intense pressure to serve the priorities of state and local elected officials. In severe weather events, for example, governors have told utilities to delay sending restoration resources to assist neighboring states until service has been restored to *all* customers (i.e., voters) in the governors' own states.

Cyber and physical attacks on the grid could create still more intense political pressure, and complicate utilities' efforts to serve national priorities versus those most urgent to meet state and local needs. Such attacks will occur in the context of broader risks of all-out war and will magnify public fears in ways that hurricanes or other natural hazards cannot—especially if those attacks are accompanied by

<sup>214</sup> Social Media Working Group for Emergency Services and Disaster Management, *Countering False Information*.

<sup>215</sup> ESCC, "ESCC: Electricity Subsector Coordinating Council."

<sup>216</sup> 16 U.S.C. § 824o-1, (b)(3).



information warfare operations to incite public panic. Governors will have powerful incentives to ensure that utilities in their states take care of their own citizens rather than meeting requests for assistance from power companies in other states.

However, from a national security perspective, not all states and customers within them will be of equal importance for protecting defense critical electric infrastructure. Some low-population states served by utilities with only limited resources are the homes of vital military installations. These utilities may need assistance from out-of-state power companies to supplement their own personnel and response capabilities when adversaries strike.

The electric industry's Cyber Mutual Assistance (CMA) Program will be critical for providing such support.<sup>217</sup> DOE is expanding the technical resources and capabilities available to support CMA response operations.<sup>218</sup> Under the national response event initiative, investor-owned utilities (led by the Edison Electric Institute) are also bolstering mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States.<sup>219</sup> All of these initiatives will be vital for responding to grid security emergencies that entail multiregional disruptions of the BPS or degrade critical electric infrastructure that the infrastructure's owners cannot restore on their own.

Yet, the voluntary nature of these mutual assistance systems could present challenges in grid security emergencies. In hurricanes or other natural hazards, governors and utilities can predict whether or not their states are likely to be struck and either husband their resources accordingly or provide them in response to requests for assistance. Cyber and physical attacks by Russia, China, or other potential adversaries are much less predictable. Enemies may

strike one region before moving on to others. Attacks could even occur on a nationwide basis. Accordingly, elected officials may discourage utility leaders from volunteering resources for mutual assistance in neighboring regions, even if their own states have not yet been struck.

Issuing emergency orders can help utilities address these challenges and serve national priorities. Participants in the Cyber Mutual Assistance Program are already taking steps to account for the risk of multiregional attacks. DOE and its industry partners should preplan to reinforce those measures in grid security emergencies. If the secretary orders utilities to help protect or restore grid reliability beyond their service areas, those orders will help justify (and indeed, legally require) providing such assistance, regardless of the political pressure against doing so. DOE should consider reaching out to state and local leaders and their senior energy appointees before emergencies occur in order to ensure that they are familiar with the FPA requirements and the national security value of mutual assistance.

Emergency orders can also help utilities execute politically unpopular emergency operational decisions within their own service areas. Cyber and physical attacks could put utility CEOs in the unenviable position of having to manage shortfalls in available power by depriving lower-priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The secretary of energy can give CEOs political top cover for taking such unpopular actions, rather than leave them to act on a voluntary basis and bear the full brunt of explaining why they did so.

Exercises can help utilities and government officials prepare to collaborate in the face of intense political pressures, and coordinate the execution of emergency orders on a nationwide basis. NERC already requires BPS entities to exercise their individual emergency and power system restoration plans. In the GridEx exercise series, over one hundred utilities across the

<sup>217</sup> ESCC, "Cyber Mutual Assistance Program."

<sup>218</sup> DOE, *Multiyear Plan*, 29.

<sup>219</sup> EEI, *Understanding the Electric Power Industry's Response and Restoration Process*.

United States and Canada test the use of their plans against combined cyber-physical attacks and exercise the use of Cyber Mutual Assistance protocols and procedures. Building template emergency orders and utility-specific implementation plans will provide an even stronger basis for coordinated multientity exercises. In planning for GridEx V in 2019, NERC and its government and industry partners should consider the possibility of exercising the issuance and implementation of specific template emergency orders. State, local, tribal, and territorial participation in utility exercises that include the use of emergency orders will also be crucial.

### Environmental, Regulatory, and Legal Waivers

In amending the FPA to address grid security emergencies, Congress provided power companies with an important protection for complying with emergency orders—one that they might not receive by implementing equivalent emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate FERC-approved grid reliability standards or other rules or provisions under the FPA, the act specifies that those actions “shall not be considered a violation” of those provisions. Such waivers of enforcement apply unless a complying entity acts in a “grossly negligent manner.”<sup>220</sup>

The FAST Act amendments to the FPA also introduced broader protections into section 202(c), absolving entities from violations of federal, state, or local environmental laws or regulations that occur as a result of complying with an order. That provision shields complying entities from “any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation.”<sup>221</sup> These protections apply to section 215A emergency orders as well.<sup>222</sup>

FPA-based waivers will be especially valuable for certain types of emergency orders. For example, if the secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service, such as proactively shedding firm load, could also violate NERC’s FERC-approved reliability standards.<sup>223</sup> Separating preplanned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards as well.

The waiver process under the FPA is structured to function automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that a BPS entity has acted with gross negligence. Nevertheless, industry, DOE, and regulators might find it useful to build consensus on the types of waivers that specific template orders should include.

Their discussions could also help address more far-reaching regulatory issues that grid security emergencies may pose. For example, the FPA does not provide waivers for Nuclear Regulatory Commission regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the commission would enforce a violation of its regulations by a nuclear generation entity complying with an emergency order. The worst time to adjudicate such a dispute, however, would be in the midst of a grid security emergency. Pre-event discussions will be particularly important given the nuclear fleet’s imperative to protect public health and safety. DOE, the Nuclear Regulatory Commission, and their industry partners will need to ensure that assessments of regulatory issues associated with

<sup>220</sup> 16 U.S.C. § 824o–1, (f)(4).

<sup>221</sup> 16 U.S.C. § 824a, (c)(3).

<sup>222</sup> 16 U.S.C. § 824o–1, (f)(2).

<sup>223</sup> For example, in events such as the September 2011 Arizona–California disturbance, FERC has found that load shedding led to violations of NERC’s reliability standards.

emergency operations take safety considerations into full account.

Preplanning will also be vital for emergency orders that support power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that “the storage of strategically located spare large power transformers” and other critical grid components “will reduce the vulnerability of the United States to multiple risks facing electric grid reliability,” including cyber and physical attacks.<sup>224</sup> Accordingly, Congress required DOE to develop a strategic transformer reserve plan to determine the number and type of spare large power transformers that should be stored and to examine issues associated with transporting those spares.<sup>225</sup>

DOE responded to this requirement by providing a strategic transformer reserve report (March 2017). The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a more substantial pool of spare large power transformers than DOE had anticipated and that a federally owned reserve is not needed.<sup>226</sup> However, the plan also found that it was crucial to ensure that large power transformers can be efficiently moved during national emergencies.<sup>227</sup>

Regulatory waivers can play a critical role in facilitating that movement. The higher-voltage classes of large power transformers, including 765-kilovolt transformers, are as big as a house and can be moved—slowly and very carefully—only by specialized heavy-haul trucks, railcars, and barges. Under the auspices of the ESCC, utilities have established the Transformer Transportation Working Group to analyze the problems posed by moving large power transformers in an emergency

and to build collaborative plans with transportation companies and associations. A central finding of the group’s analysis: regulatory waivers will be critical to expedite the movement of large power transformers, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.<sup>228</sup>

DOE’s 2017 transformer report committed the department to coordinating with the Transformer Transportation Working Group “to improve and optimize transportation planning in response to a significant national event impacting the electricity grid.”<sup>229</sup> However, the report did not examine how emergency orders and implementation plans might speed the transportation of large power transformers. As DOE collaborates with the working group and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols that are not addressed by the FPA and that pose the greatest impediments to transformer movement. DOE and its partners should then preplan to waive these provisions if the secretary issues emergency orders.

The challenge for such preplanning: the secretary of energy lacks the statutory authority to waive key transportation regulations. Most federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of DOT. Federal regulations and emergency operations that would govern the movement of transformers on barges, which could be critical for restoring power for coastal cities and along the Mississippi–Ohio river system of inland waterways, are overseen by the US Coast Guard and the US Army Corps of Engineers. State and local transportation regulations and permitting requirements will also

---

<sup>224</sup> FAST Act, 1779.

<sup>225</sup> FAST Act, 1780–1782.

<sup>226</sup> DOE, *Strategic Transformer Reserve*, 21.

<sup>227</sup> DOE, *Strategic Transformer Reserve*, 1.

---

<sup>228</sup> ICF, *Assessment of Large Power Transformer Risk Mitigation Strategies*, 22–23.

<sup>229</sup> DOE, *Strategic Transformer Reserve*, 22.

pose major impediments to moving large power transformers over roads unless adequate waivers are in place to lift restrictions.

DOE should build collaborative plans to employ waiver authorities beyond those directly under the secretary's control. For example, to facilitate the movement of large power transformers, gubernatorial disaster declarations could help waive state-level regulations. The American Association of State Highway and Transportation Officials and National Emergency Management Association are exploring the use of these and other waiver authorities. DOE is also preplanning with other federal, state, local, tribal, and territorial agencies to coordinate response operations under Emergency Support Function #12—Energy.<sup>230</sup> Especially valuable, a growing number of individual power companies are creating contingency plans for emergency transportation with government agencies and road, rail, and barge companies. Building on these efforts, and on initiatives led by the Transformer Transportation Working Group,<sup>231</sup> the electricity subsector and its partners should establish systematic, nationwide plans to facilitate the movement of transformers and other critical equipment in grid security emergencies.

Over the longer term, Congress, industry, and government partners should also consider whether complying entities should have liability protections beyond those currently provided by the FPA. Prioritized load shedding for extended periods will create “winners and losers” in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other section 9+ assets may leave shortfalls in electric service at dialysis centers, small urgent-care centers, and facilities for special-needs citizens. These disruptions will put lives at risk. Legislators, DOE, and electric industry leaders should examine whether utilities complying

with such necessary but highly disruptive emergency orders ought to have additional liability protections. Cutting off power to lower-priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.<sup>232</sup> Again, if these risks of exposure are sufficiently severe, Congress should consider providing further protections for BPS entities.

### **Cost Recovery for Emergency Operations and Support for Investments in Grid Infrastructure**

Complying with emergency orders may force utilities to incur costs beyond their normal operating expenses. The FPA states that if FERC determines “that owners, operators, or users of critical electric infrastructure have incurred substantial costs” in complying with an emergency order, FERC shall “establish a mechanism that permits such owners, operators, or users to recover such costs.”<sup>233</sup> Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other orders could require reimbursement through FERC-directed mechanisms as well.

The act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that emergency orders require utilities responsible for defense critical electric infrastructure to take emergency measures, the “owners or operators” of critical defense facilities that rely on such infrastructure “shall bear the full incremental costs of the measures.”<sup>234</sup> Fair warning to DOD: it

<sup>230</sup> “State and Local Energy Assurance Planning.” DOE.

<sup>231</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>232</sup> Frankel, “Can Customers Sue Power Companies for Outages?”

<sup>233</sup> The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs “prudently” and that those costs “cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users.” 16 U.S.C. § 824o–1, (b)(6)(A).

<sup>234</sup> 16 U.S.C. § 824o–1, (b)(6)(B).



should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- attacks create major blackouts and deprive utilities of revenue;
- emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- adversaries disrupt financial markets, either through direct cyber attacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.<sup>235</sup>

Power companies are strengthening their plans and capabilities for cross-sector support with the financial services sector.<sup>236</sup> These efforts should include the development of contingency plans for financial-services companies (in coordination with the Department of Treasury and DOE) to help utilities cover the urgent expenses they may incur in responding to grid security emergencies. In addition, to facilitate the reimbursement process provided for in the FPA, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with orders will be more difficult once attacks are under way.

Cost recovery for investments in grid infrastructure to facilitate emergency order implementation will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. Other orders may be impossible to execute unless BPS entities make additional investments in infrastructure. It will be near useless to order transmission operators to protect or rapidly restore service to vital but remote military bases served by a single transmission line if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure that these facilities can help defeat US adversaries when the nation is under attack. DOD will need to develop a cost-recovery mechanism to reimburse defense critical electric infrastructure owners for making such investments.

To be even remotely viable as an emergency order design option, most preplanned power islands will also require at least some infrastructure construction. Ideally, these preplanned islands will use existing generation, transmission, and distribution assets within their service footprints to separate from the grid and still be able to provide reliable electric service to the section 9+ assets inside their borders. But many areas that might be designed to function as islands in a grid security emergency will lack adequate infrastructure to do so. The grid's interconnected design enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Preplanned power islands will not only lose those reliability benefits, but they will also have to make do with infrastructure that utilities built and aligned to be supporting components of the interconnected grid—*not* self-sustaining islands that would be stood up in grid security emergencies. Moreover, operating and recovering from preplanned island schemes will create an entirely different operating mode than industry is currently designed

<sup>235</sup> NERC, *GridEx III Report*, 15.

<sup>236</sup> See, for example, the Strategic Infrastructure Coordinating Council (SICC). ESCC, "ESCC: Electricity Subsector Coordinating Council."



for. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: to be effectively implemented, many emergency orders could require spending on new transmission lines and other grid infrastructure.

The FPA provisions for grid security emergencies do not explicitly authorize reimbursement for infrastructure investments. While the act requires FERC to establish a mechanism to enable owners, users, and operators of critical and defense critical electric infrastructure to recover their costs of complying with emergency orders, those funding provisions do not mention preattack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover costs for infrastructure investments in resilience against cyber and physical attacks.<sup>237</sup> FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate emergency order execution.

Similar discussions will be necessary with state public utility commissions. As noted above, local distribution systems will play vital roles in implementing emergency orders. Public utility commissions have primary regulatory authority over such distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. They could also make important contributions to reviewing proposed implementation plans for emergency orders that would be executed within their respective states, particularly when local distribution systems would be necessary to implement the orders.

<sup>237</sup> See, for example, FERC, *Extraordinary Expenditures* (96 FERC ¶ 61,299), 1; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), 10–11; and FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), 60.

The FPA opens the door to such discussions. The act states that FERC and the secretary of energy “shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions.”<sup>238</sup> Initiating these discussions with the National Association of Regulatory Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has extensively analyzed criteria for assessing the prudence of investments against cyber and physical attacks and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

## Conclusions and Recommendations for Broader Progress

Taken together, the options for industry–government collaboration examined in this report constitute a massive undertaking for which Congress appropriated zero funding to utilities. Developing a sequenced, prioritized strategy to explore these options will help make doing so a more manageable task.

Potential emergency orders will differ not only in terms of the phases of an attack in which they would be most useful, and in the degree to which they will disrupt normal electric service, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create—especially those that fall into the no-regrets category. Utilities frequently use conservative operations to help protect grid reliability in severe weather events. A growing number of companies are

<sup>238</sup> 16 U.S.C. § 824o–1, (d)(4).

already building on that foundation to draft equivalent conservative operations against cyber and physical threats. Emergency orders based on these initiatives constitute “low-hanging fruit”; creating such orders offers an immediate opportunity for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging emergency order initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are under way, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. Improving communications survivability and preplanning to counter disinformation campaigns will also be crucial for grid security emergency preparedness. So, too, will be efforts not only to fully leverage the FPA’s regulatory waiver and cost recovery mechanisms but also to explore additional liability protections and other measures to help entities comply with emergency orders.

A comprehensive plan to align and integrate these initiatives should also address three additional opportunities to build resilience for grid security emergencies: (1) preplanning to use additional federal and state emergency authorities to defend natural gas systems, communications networks, and other infrastructure on which the grid depends; (2) coordinating with Canada, Mexico, and other nations whose grids may be struck in conjunction with attacks on US electric systems; and (3) exploring new options to deter and defeat attacks on the grid by integrating defensive measures with government operations to blunt further strikes on US power companies and other targets.

## Employing Additional Emergency Authorities for Cross-Sector Resilience

Building preparedness against attacks on the grid is necessary but not sufficient to protect BPS reliability. In many US regions, power generation is becoming extraordinarily dependent on the flow of natural gas. Adversaries may attempt to cause cascading blackouts and other major grid instabilities by crippling natural gas systems. To hedge against such disruptions, some generators have the ability to operate on diesel and other secondary fuels if attackers interrupt gas supplies. But the refining and transportation systems needed to resupply such “dual-fuel” generators with diesel will themselves be at risk in grid security emergencies.<sup>239</sup> Moreover, as examined earlier in this report, coordinated grid restoration will also depend on the availability of communications systems and other infrastructure sectors.

This report has focused on employing the emergency authorities that Congress incorporated into the FPA by creating section 215A of the act in 2015. However, these authorities apply only to BPS owners and operators. The secretary cannot issue emergency orders under 215A to operators of natural gas and diesel fuel systems, much less to telecommunications companies and other infrastructure owners beyond the energy sector. The secretary has a range of other emergency authorities, including the Defense Production Act (DPA) and the authorities provided by section 202(c) of the FPA, which could facilitate coordinated response and restoration operations across the energy sector. The analysis that follows examines how DOE and its industry partners could preplan for the integrated use of all such authorities in a grid security emergency. This analysis also examines how federal and state leaders might use additional emergency powers to coordinate multisector response operations.

---

<sup>239</sup> The author has advised Exelon Corporation on risks of fuel interruptions for power generation. Exelon has provided no funding for this report.

## Coordinating Emergency Operations among Electric Utilities, Natural Gas Systems, and Other Energy Sector Components

Natural gas is an increasingly important source of fuel for power generation in many regions of the United States. Between 2002 and 2016, the nationwide share of electricity provided by gas-fired units increased from 18 percent to approximately 34 percent.<sup>240</sup> However, in New England, California, and other parts of the United States, natural gas has become the predominant source of fuel for power generation.

ISO New England has highlighted the risks that this reliance creates for grid resilience. It notes that “in New England, the most significant resilience challenge is fuel security—or the assurance that power plants will have or be able to obtain the fuel they need to run, particularly in winter—especially against the backdrop of coal, oil, and nuclear unit retirements, constrained fuel infrastructure, and the difficulty in permitting and operating dual-fuel generating capability.”<sup>241</sup>

Other regions also face growing fuel supply risks to grid resilience. A DOE-sponsored report titled *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units, Volume I: The Critical Role of Thermal Units During Extreme Weather Events* (March 2018) notes that many regional transmission organizations and independent system operators will face a combined challenge of inadequate natural gas pipeline infrastructure and competing demands for fuel from users apart from power generators.<sup>242</sup> More broadly, NERC has found that “the electric sector’s growing reliance on natural gas raises concerns regarding the ability to maintain BPS reliability when facing constraints on the natural

gas delivery systems.”<sup>243</sup> NERC’s 2016 *Long-Term Reliability Assessment* also notes that “as part of future transmission and resource planning studies, planning entities will need to more fully understand how impacts to the natural gas transportation system can impact electric reliability.”<sup>244</sup> Additionally, in *Grid Resilience in RTOs and ISOs* (January 2018), FERC called for additional data to better assess the risks posed by “wide-scale disruption to fuel supply” that could result in outages of multiple generators.<sup>245</sup>

Companies in the oil and natural gas subsector are bolstering their capabilities to protect their critical system components from attack and are taking new measures to ensure the continued safe and reliable delivery of natural gas to critical customers, including power generators.<sup>246</sup> However, threats to the oil and natural gas subsector are rapidly escalating as well.<sup>247</sup> As gas system owners and operators address these increasing threats, new opportunities will emerge for joint gas–electric resilience initiatives and emergency planning.

The oil and natural gas and electricity subsectors are already improving their coordination on resilience issues.<sup>248</sup> Moreover, NERC has been facilitating coordination between BPS entities and natural gas companies to address fuel resilience and interdependency challenges.<sup>249</sup> The ESCC has also been developing new coordination mechanisms for the

<sup>243</sup> NERC, *Short-Term Special Assessment*, 12. See also NERC, *2013 Special Reliability Assessment*.

<sup>244</sup> NERC, *2016 Long-Term Reliability Assessment*, 21.

<sup>245</sup> FERC, *Grid Resilience*, 161 FERC ¶ 61,012 (2018), 14. See also Stockton, *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*.

<sup>246</sup> “Cybersecurity,” American Gas Association.

<sup>247</sup> Sobczak, Northey, and Behr, “Cyber Raises Threat”; and Stockton (on behalf of Exelon Corporation), *Prepared Direct Testimony* (Docket No. RM18-1-000), 13.

<sup>248</sup> DOE, *Staff Report to Secretary*, 94; and EIS Council, *E-PRO Handbook II*, 189.

<sup>249</sup> NERC, *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*, 1.

<sup>240</sup> DOE, *Staff Report to Secretary*, 90.

<sup>241</sup> ISO-NE, “Response of ISO New England Inc.,” 1.

<sup>242</sup> NETL, *Reliability, Resilience and the Oncoming Wave*, 4, 14, 22, 3.

two industries (as well as with communications and financial services sectors).<sup>250</sup> Additionally, the natural gas industry participated in GridEx IV, which examined opportunities to mitigate the risk that adversaries will simultaneously attack gas and electric systems.

Building on these and other collaborative efforts, gas and electric companies (and their regulatory partners) should examine how they can prioritize support for each other in grid security emergencies. For example, when blackouts occur, electric companies typically prioritize the restoration of service to compression stations and other electricity-dependent gas infrastructure that is essential to supply fuel for power generation and other critical customers. Support for gas infrastructure should remain a priority, even as BPS entities add other section 9+ facilities to their restoration plans. Gas companies might also reassess their curtailment policies to help gas-dependent BPS entities sustain service to major military installations and other vital facilities in grid security emergencies.<sup>251</sup>

BPS entities and DOE should also pursue deeper collaboration with the companies that refine and deliver secondary fuels for power generation. If adversaries interrupt the flow of natural gas, dual-fuel generators can use diesel, no. 2 fuel oil, or other secondary fuels to sustain their operations in a grid security emergency.<sup>252</sup> However, cascading blackouts could disrupt the flow of these secondary fuels as well. Refining and transportation systems components that are essential to resupply dual-fuel generators depend on electricity. Adversaries may also attack these systems at the same time they strike the grid. Moreover, ongoing cutbacks in industry delivery capacity could magnify these risks of interruption. ISO New England notes that a “withering

delivery supply chain” constitutes an “unquantifiable X factor” in assessing grid resilience.<sup>253</sup> Preplanning to prioritize the delivery of secondary fuels for power generation will be essential for grid security emergencies, especially given the enormous demand for diesel from emergency power generators from hospitals, water utilities, and other vital facilities in wide-area blackouts.

Emergency authorities beyond 215A can help prioritize the flow of natural gas and secondary fuels to protect and restore grid reliability. The DPA will be especially helpful in this regard. The act is the “primary source of presidential authority to expedite and expand the supply of critical resources from the U.S. industrial base to support the national defense and homeland security.”<sup>254</sup> The DPA defines national defense to include “critical infrastructure protection and restoration,” encompassing all electric system components and supporting fuel supply infrastructure (including natural gas pipelines) that are at risk of cyber and physical attacks.<sup>255</sup> In 2012, the White House delegated many of the president’s DPA authorities to the heads of relevant federal agencies, including the secretary of energy for prioritization and allocation decisions regarding “all forms of energy.”<sup>256</sup>

Especially valuable for cross-sector resilience, DOE has established an Energy Priorities and Allocations System that enables the department to prioritize contracts for the delivery of natural gas, diesel, and other energy resources between the companies that provide them and government agencies, electric utilities, and other private and public sector customers. The system also enables DOE to allocate energy materials, services, and facilities to promote

<sup>250</sup> ESCC, “ESCC: Electricity Subsector Coordinating Council.”

<sup>251</sup> EIS Council, *E-PRO Handbook II*, 219.

<sup>252</sup> ISO-NE, *Operational Fuel-Security Analysis*, 52; and NERC, *2013 Special Reliability Assessment*, 4.

<sup>253</sup> ISO-NE, *Operational Fuel-Security Analysis*, 14, 16.

<sup>254</sup> DHS, *Power Outage Incident Annex*, 129.

<sup>255</sup> 50 U.S.C. § 4552, (14).

<sup>256</sup> Obama, *Executive Order—National Defense Resources Preparedness*.



“critical infrastructure protection and restoration” and emergency preparedness.<sup>257</sup>

DOE has already used its authorities under the DPA to support power generation in previous energy crises. In 2001, for example, the department used these authorities to ensure that emergency supplies of natural gas continued to flow to Californian power generators, thereby helping to avoid threatened electrical blackouts.<sup>258</sup> Now, to build preparedness for grid security emergencies, DOE and its industry partners should consider preplanning to use the DPA to sustain or restore gas and diesel deliveries to critical generators, including those that serve microgrids on defense installations, regional hospitals, and other assets critical for national security and public health and safety.

DOE could use the DPA to support and prioritize power restoration operations in other ways as well. Section 101(a) of the act provides DOE with the authority to prioritize the delivery of critical grid components in an emergency. If coordinated physical attacks damage or destroy transformers at a large number of critical substations, the secretary could use the DPA to allocate replacement transformers in ways that most directly benefit national security and public health and safety.

Two additional sources of emergency authorities could further strengthen preparedness and supplement the use of section 215A emergency orders. The first is section 202(c) of the FPA. The section authorizes the secretary to order “temporary connections of facilities and such generation, delivery, interchange, or transmission of electric energy as in its judgment will best meet the emergency and serve the public interest.” That provision also specifies that the secretary could exercise such powers “during the continuance of any war in which the United States is engaged, or whenever the Commission determines that an

emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy or of facilities for the generation or transmission of electric energy, or of fuel or water for generating facilities, or other causes.”<sup>259</sup>

A key virtue of section 202(c) is that the secretary can apply these emergency authorities to local distribution systems that might not fall within the purview of section 215A. Moreover, DOE has a strong record of having used 202(c) authorities in past emergencies, including the California Enron crisis, Hurricane Katrina, and other events.<sup>260</sup> DOE and its industry partners should consider building on this foundation to plan for the use of these authorities in grid security emergencies.

The Natural Gas Policy Act provides further authorities that could help coordinate energy sector operations in grid security emergencies. The president must declare a natural gas supply emergency before the secretary gains emergency powers under the act. The president can make such a declaration if there is evidence of an imminent or existing “severe natural gas shortage, endangering the supply of natural gas for high-priority uses” and that, having exhausted other alternatives “to the maximum extent practicable,” natural gas emergency authorities are necessary to resolve the situation.<sup>261</sup> The president may also delegate this authority, as well as the authority to issue rules or orders, to the secretary of energy or other appropriate federal officials.<sup>262</sup>

The president or secretary can issue two main types of orders or rules. Most important, during a natural gas supply emergency, the act authorizes the president or other officials to allocate natural gas supplies “to assist in meeting natural gas requirements for high-priority

<sup>257</sup> DOE, “RIN 1901-AB28,” 33615, 33622-33626.

<sup>258</sup> Brown and Else, *Defense Production Act of 1950*, 10.

<sup>259</sup> 16 U.S.C. § 824a, (c)(1).

<sup>260</sup> “DOE’s Use of Federal Power Act Emergency Authority,” DOE.

<sup>261</sup> 15 U.S.C. § 3361, (a).

<sup>262</sup> 15 U.S.C. § 3364, (d).



uses.”<sup>263</sup> The secretary could use this provision to ensure that critical generating facilities get the fuel they need.

Of course, some of these authorities overlap. DOE and its government and industry partners should develop an integrated approach to employing these powers for grid security emergencies, and determine which particular authorities are best suited to meet specific energy sector risks that cyber and physical attacks can create. These partners, along with other energy sector stakeholders, should also consider exercise scenarios that involve the simultaneous use of multiple emergency authorities to simulate the complex legal environment they may be faced with in a grid security emergency.

### **Multisector Resilience for Grid Security Emergencies**

An overarching strategy for grid security emergency preparedness should also advance operational coordination between energy companies and other infrastructure sectors that both rely on electricity and play vital roles in power restoration. Additional federal emergency authorities and incident response plans can help strengthen coordination between these interdependent sectors.

Using this broader array of plans and authorities will be particularly important if adversaries simultaneously attack multiple infrastructure sectors. By striking other sectors together with the grid, adversaries can exploit interdependencies between them to maximize the attack’s disruptive effects on national security, including the ability of defense installations and supporting civilian infrastructure to conduct operations abroad.<sup>264</sup> The *National Cyber Incident Response Plan* provides a framework for strengthening multisector coordination mechanisms for such attacks. As the administration refines the

plan, DOE and its government and industry partners should ensure that the issuance and execution of emergency orders fit within this broader framework and directly contribute to multisector resilience.

Updates to the *National Response Framework* and other FEMA-led initiatives can offer further benefits for grid security emergencies. In its after-action report from the 2017 hurricane season, FEMA noted that emergency managers and their private sector partners lack the multisector coordination mechanisms necessary to accelerate the restoration of electric power and other lifeline services.<sup>265</sup> The report called for FEMA to build “a cross-sector approach to the Agency’s planning, organizing, response, and recovery operations,” and revise current national-level planning frameworks to create a cross-sector emergency support function.<sup>266</sup> DOE and industry should partner to prioritize support for power sustainment and restoration within this broader initiative.

The *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans* provides a prime opportunity to embed cross-sector coordination efforts in regional incident response plans.<sup>267</sup> The annex calls for the development of regional plans to build resilience against extended multistate blackouts and ensure that interdependent sectors can accelerate power restoration while also countering threats to public health and safety.<sup>268</sup> In many areas of the United States, utilities are already helping DOE, FEMA, and their state and local partners build such plans for their regions. Cross-sector preparedness for grid security emergencies should become a key focus of future power outage incident planning efforts.

<sup>263</sup> 15 U.S.C. § 3363, (a).

<sup>264</sup> Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee*, 11.

<sup>265</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 13.

<sup>266</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 12–13.

<sup>267</sup> EIS Council, *E-PRO Handbook III*, 45.

<sup>268</sup> DHS, *Power Outage Incident Annex*, 77.

In all of these planning and operational coordination initiatives, DOE and other departments responsible for specific infrastructure sectors should examine how other federal emergency authorities might supplement those that apply to the energy sector. The communications sector provides one such opportunity. The president has extensive authorities to address national security and emergency preparedness telecommunications issues under the Communications Act, including the power to prioritize the use of communications capabilities and provide complying entities with legal and regulatory protections.<sup>269</sup> Executive Order 13618 assigns many of these authorities and associated responsibilities to federal departments and agencies. The secretary of commerce, for example, is responsible for developing plans and procedures for emergency use of radio frequencies and other communications systems.<sup>270</sup> The secretary of homeland security is responsible for overseeing the development, testing, and implementation of emergency communications capabilities.<sup>271</sup> Using these capabilities to support power restoration could be enormously helpful in grid security emergencies. Equivalent emergency authorities for other sectors could assist restoration as well. However, as with all such opportunities, effectively using these federal authorities will depend on extensive preplanning.

State governors are likely to invoke their own authorities to respond to grid security emergencies. Governors have primary responsibility for protecting the health and safety of their citizens. Cyber and physical attacks on the grid, especially if paired with strikes against communications systems and other interdependent sectors, could disrupt hospitals, water systems, and other assets on which their citizens rely. Governors in every state have the ability to declare emergencies and issue executive orders to help deal

with such threats to public health.<sup>272</sup> A growing number of states are also including utility representatives in their emergency operations centers, building collaborative plans and coordination mechanisms to respond to attacks on the grid, and preparing for state National Guard personnel to help utilities defend and restore the flow of power. These initiatives are bolstering overall preparedness for grid security emergencies. However, if multiple governors employ their own emergency authorities and implement state-level blackout response plans, it will be enormously difficult to coordinate their efforts with federal actions—including the issuance of DOE emergency orders to utilities in those very same states.

The only way to overcome such difficulties is to exercise the use of all of the authorities that could help protect and restore grid reliability, across multiple sectors and with the participation of both federal and state leaders. GridEx IV offered an important step forward in this regard. Exercise participants from the oil and natural gas subsector, as well as the financial-services and communications sectors, contributed perspectives on how they could help utilities respond to cyber and physical attacks on the grid. Representatives from state governments discussed how governors might act in such an emergency. GridEx V will provide an opportunity to address such coordination challenges in greater detail. GridEx V could also exercise the use of specific template emergency orders, together with communications mechanisms and playbooks developed for grid security emergencies. Additional exercises by BPS entities and their partners at all levels of government will also be vital to prepare for the implementation of such orders.

## Extended Partnership Requirements within the United States and Abroad

Congress implicitly imposed geographic constraints on the secretary's authority to issue emergency orders to protect the reliability of defense critical electric

<sup>269</sup> 47 U.S.C. § 606.

<sup>270</sup> Obama, *Executive Order—Assignment*, section 5.3.

<sup>271</sup> Obama, *Executive Order—Assignment*, section 5.2. See also DHS, “Emergency Communications.”

<sup>272</sup> Orenstein and White, “Emergency Declaration Authorities.”

infrastructure. The FPA limits such infrastructure to that which is located in the forty-eight contiguous states or the District of Columbia.<sup>273</sup> However, Alaska and Hawaii are home to vital grid-dependent military installations and supporting civilian infrastructure, including facilities for US continental ballistic missile defense and command and control of military operations in the Pacific region. Key defense installations also exist in Guam and other US territories. As the electric industry and DOE build preparedness for grid security emergencies, they should consider collaborating with the utilities that serve these states and territories and their government partners (including DOD) to strengthen plans and capabilities for coordinated operations.

Close coordination will also be necessary with Canada. The secretary of energy has no authority to issue emergency orders to power companies in other countries. However, the electric grids of the United States and Canada are deeply interconnected. This integration entails both risks and opportunities in grid security emergencies. Adversary-induced blackouts in one nation may cascade across the border, and extraordinary measures taken to restore US grid reliability could affect Canadian systems. Yet, the connectivity between US and Canadian electric systems can also provide unique opportunities to strengthen the security and emergency preparedness of both nations.

A key foundation for binational cooperation in grid security emergencies is already in place. NERC's reliability standards apply to both US and Canadian utilities, providing shared planning and emergency coordination mechanisms on both sides of the border. US and Canadian power companies and government officials should explore how they might supplement these existing mechanisms for

grid security emergencies. The most immediate opportunity to do so will lie in government-to-government consultations. The FPA requires that, to the extent practicable, the secretary of energy shall consult with Canadian authorities before issuing emergency orders.<sup>274</sup> However, the FPA provides no details on the mechanisms by which consultations will be conducted or on whether and how Canadian officials should be informed when the secretary issues emergency orders to US utilities. The analysis that follows examines opportunities to facilitate binational consultation and operational coordination in grid security emergencies.

The FPA also requires that the secretary consult with the Mexican government before issuing emergency orders. While the US and Mexican grids are much less integrated than those of the US and Canada, discussions on grid security emergency preparedness with Mexican officials could also be valuable. Coordination beyond North America may be useful as well. If a severe regional crisis escalates into attacks on the US power grid, US security partners in those regions may face strikes against their own electric systems. Sharing information on whether an attack is imminent and taking coordinated grid protection measures (including those for conservative operations) will help the United States and its allies meet such challenges.

### **Deepening Integration between US and Canadian Grids: Risks and Potential Benefits for Grid Security Emergency Resilience**

DOE notes that "the United States and Canada serve as a global model of highly functional, cross-border electricity coordination."<sup>275</sup> US and Canadian grids are connected by over three dozen major transmission lines, ranging from the Pacific Northwest to New England. The resulting power flows have created a deeply integrated network of north-south BPS infrastructure and synchronized

<sup>273</sup> 16 U.S.C. § 824o-1, (a)(4). The FPA's section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).

<sup>274</sup> 16 U.S.C. § 824o-1, (b)(3).

<sup>275</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-5.

cross-border operations.<sup>276</sup> This integration also provides significant economic and energy security benefits for both countries.<sup>277</sup>

Connectivity between US and Canadian grids will grow still closer in the decades to come.<sup>278</sup> New York and Massachusetts are pursuing significant increases in Canadian hydropower to help achieve their clean energy goals. Several new cross-border transmission lines are also under development, though many of them face permitting challenges. The Lake Erie Connector is a one-thousand-megawatt high-voltage, direct current line expected to link Ontario's Independent Electricity System Operator with PJM in 2020.<sup>279</sup> The Champlain Hudson Power Express from Quebec to New York City is expected to go into service in 2021, with still other projects in various phases of development in New England, the Midwest, and the Pacific Northwest.<sup>280</sup>

These and other projects offer significant economic benefits to both nations. However, the connectivity of US and Canadian power grids also creates risks of cross-border failures. The 2003 Northeast blackout that started in Ohio created power outages for millions of customers in Ontario.<sup>281</sup> Interconnections between US and Canadian power systems have increased since that event. US and Canadian officials warn that given this connectivity, "isolated or complex events with cascading effects that take place in either country can have major consequences for both the United States' and Canada's electric grids and adversely affect national security, economic stability, and public health and safety."<sup>282</sup>

<sup>276</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-6.

<sup>277</sup> Stanley, *Mapping the U.S.-Canada Energy Relationship*, 9.

<sup>278</sup> Parfomak et al., *Cross-Border Energy Trade*, 34.

<sup>279</sup> "Work Continues on ITC Lake Erie Project," *Transmission Hub*.

<sup>280</sup> Vine, *Interconnected: Canadian and U.S. Electricity*, 9.

<sup>281</sup> NERC Steering Group, *Technical Analysis of Blackout*, 1.

<sup>282</sup> Governments of US and Canada, *Joint United States-Canada Electric Grid Security and Resilience Strategy*, 10.

Mandatory reliability standards reduce the risks of outages across North America. In the aftermath of the 2003 blackout, NERC began issuing standards applicable to entities on both sides of the border. NERC reliability standards are mandatory and enforceable in the provinces of Ontario, New Brunswick, Alberta, British Columbia, Manitoba, and Nova Scotia. Twelve such reliability standards also went into effect in Quebec in April 2015; the province is now considering adopting additional standards.<sup>283</sup> These shared US-Canada standards help power companies in both countries maintain the reliability of their systems and will help them prevent instabilities from spreading during grid security emergencies.

NERC's role as the electric reliability organization for North America provides an additional bulwark for binational grid resilience. As Figure 7 illustrates, three NERC regional entities include power companies on both sides of the border: the Northeast Power Coordinating Council (NPCC), the Midwest Reliability Organization (MRO), and the Western Electricity Coordinating Council (WECC). These entities help monitor and enforce compliance with reliability standards and reinforce NERC's integrated approach to reducing the risks of cascading failures and other instabilities.<sup>284</sup> The E-ISAC also provides additional support for utility preparedness in both nations.

However, Russia and other potential adversaries' increasingly sophisticated cyber capabilities pose challenges for protecting power flows between Canada and the United States, just as they do for electric service within each country individually.

Connectivity between US and Canadian power systems offers other benefits for protecting reliability against cyber and physical attacks. For example, as

<sup>283</sup> "North America," NERC. See also "Compliance - Québec," Northeast Power Coordinating Council; and "Electric Power Transmission Reliability Standards," Régie de l'énergie Québec.

<sup>284</sup> "Key Players," NERC.



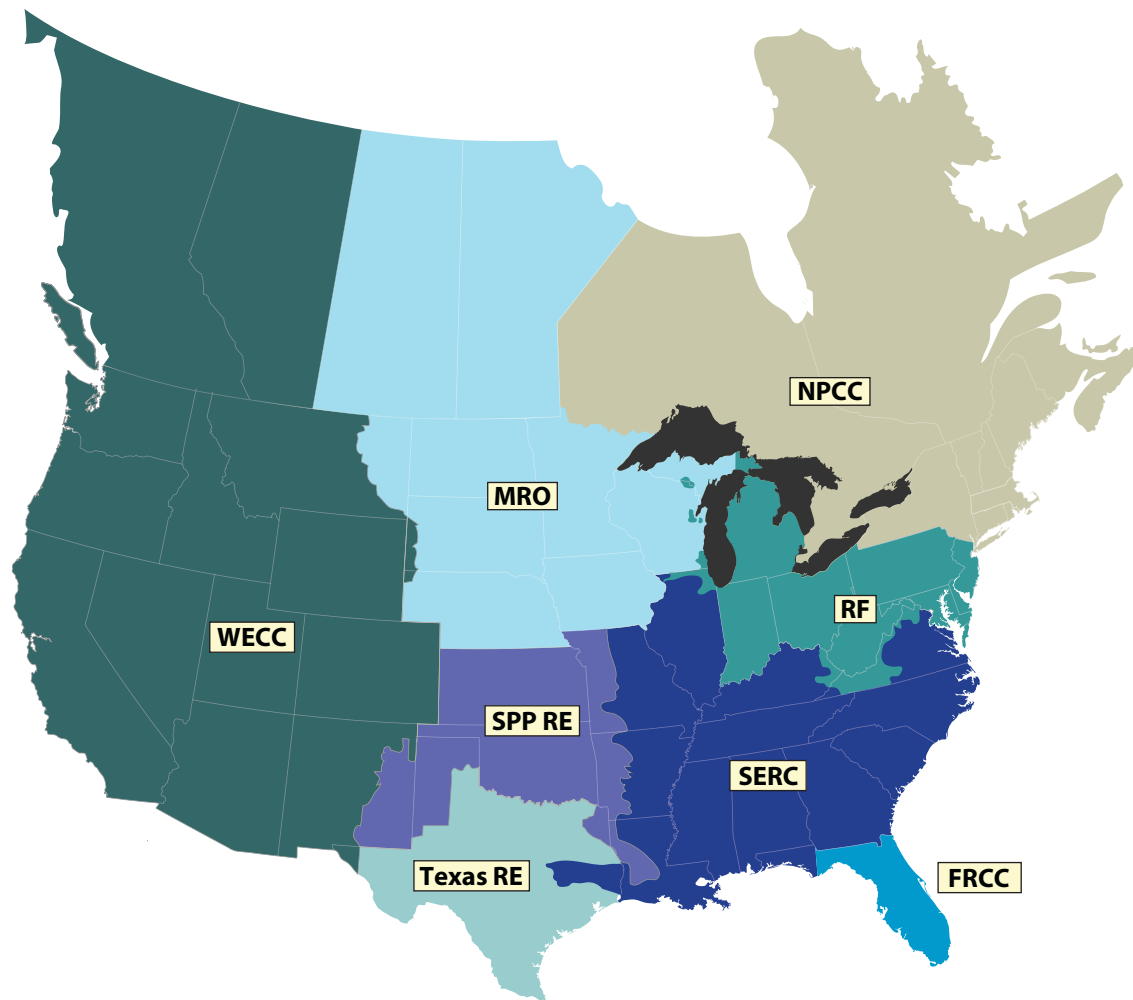


Figure 7. NERC Regional Entities across North America

new transmission lines increase this connectivity, electricity exported by Canada could become increasingly valuable when managing power imbalances in the United States and could make up for sudden shortfalls in the availability of US-generated power. However, we must assume that adversaries know this as well. To maximize the disruption to the US grid and the critical facilities that depend on it, attackers may strike the cross-border transmission lines that would otherwise help US grid owners and operators prevent cascading failures, uncontrolled separations, and other major reliability issues.

Adversaries may also attack grid assets that supply power to critical Canadian defense installations. The United States and Canada have a unique binational

defense system to protect their territories. The North American Aerospace Defense Command plays a vital role for both nations for aerospace warning, aerospace control, and maritime warning for North America.<sup>285</sup> The Canada-US Civil Assistance Plan also helps enable military members from one nation assist the other's armed forces in support of civilian authorities during emergencies.<sup>286</sup> Potential adversaries such as Russia may seek to degrade these binational military capabilities and operations by attacking defense critical electric infrastructure on

<sup>285</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

<sup>286</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.



both sides of the border. US and Canadian officials and power companies should plan accordingly for mutual support in grid security emergencies.

### Specific Options for US–Canada Coordination

In addition to requiring US–Canada consultations before the secretary issues emergency orders, the FPA also states that FERC and the secretary “shall, in consultation with Canadian and Mexican authorities, develop protocols for the voluntary sharing of critical electric infrastructure information with Canadian and Mexican authorities and owners, operators and users of the bulk-power system outside the United States.”<sup>287</sup> Those initiatives provide a valuable starting point to build shared North American preparedness for grid security emergencies. However, much deeper collaboration is both possible and necessary, especially with Canada. Options for further analysis are described below.

**Consultative mechanisms, collaborative planning, and coordinated emergency operations.** The FPA does not specify how US officials would consult with their Canadian counterparts if the president declares a grid security emergency. Nor does it discuss whether the president would do so prior to making such a declaration. Exchanges between the US president and the prime minister of Canada would constitute the highest level of binational coordination. More detailed discussions about options for responding to incidents could also occur between the secretary of energy and the Canadian minister of national resources. That minister has the federal lead for electricity issues in Canada but lacks emergency authorities equivalent to those that the FPA grants to the secretary of energy.<sup>288</sup>

However, government coordination mechanisms will also need to include a broader array of participants. Global Affairs Canada and the US State Department might well be involved in any coordination of

binational grid emergency actions, just as they are in other emergency assistance mechanisms.<sup>289</sup> Coordination with state and provincial governments could also be helpful. The 1982 amendments to Canada’s Constitution Act (1867) explicitly recognized provinces’ and territories’ constitutional rights to manage electrical energy.<sup>290</sup> In particular, authority over electricity generation and transmission in Canada rests primarily with provincial governments.<sup>291</sup> It will be essential to account for these features of Canadian governance in building US–Canada consultative mechanisms.

The NERC alert system and other emergency coordination systems provide a solid basis for collaboration between US and Canadian utilities in grid security emergencies. However, the FPA does not address the question of how (and how much) information DOE officials should share with Canada on the issuance of emergency orders to US utilities. Given the deep integration of the US and Canadian grids, maximum sharing could help coordinate both countries’ emergency operations before, during, and after attacks. To facilitate such information sharing, DOE, Natural Resources Canada, and other relevant stakeholders can leverage existing US–Canadian mechanisms to protect sensitive information, supplemented as needed to support grid security emergency coordination.

The *Joint US-Canada Electric Grid Security and Resilience Strategy* (December 2016) provides a policy framework for building these coordination and information sharing mechanisms. The US and Canadian governments developed the strategy “to strengthen the security and resilience of the U.S. and Canadian electric grid from all adversarial, technological, and natural hazards and threats.”<sup>292</sup> The strategy calls for collaboration to protect system assets and

<sup>287</sup> 16 U.S.C. § 824o–1, (d)(5).

<sup>288</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>289</sup> “Compendium,” Public Safety Canada.

<sup>290</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>291</sup> “North America,” NERC.

<sup>292</sup> Governments of US and Canada, *US-Canada Electric Grid Security and Resilience Strategy*, 1.

critical functions in both nations so that the North American grid can “withstand and recover rapidly from disruptions.”<sup>293</sup> The strategy also emphasizes the need for collaboration to manage contingencies and enhance response and recovery efforts.<sup>294</sup> All of these features make the strategy a promising basis for creating the detailed collaborative mechanisms that grid security emergencies will require.

### **Protecting defense critical electric infrastructure.**

While the FPA facilitates the development of emergency orders to protect the flow of power to critical US defense installations, US–Canada coordination in grid security emergencies could also help strengthen power resilience for bases on both sides of the border. The Pacific Northwest exemplifies the potential benefits of such collaboration. Washington State hosts a number of vital installations, including Joint Base Kitsap on Puget Sound, which serves as the homeport for aircraft carriers, attack submarines, and other assets that would be needed for operations in the South China Sea and for other regional contingencies. Canadian Forces Base Esquimalt and other key Canadian installations are located less than one hundred miles away on Vancouver Island. Esquimalt is the second-largest military base in Canada and is home to Maritime Forces Pacific and Joint Task Force Pacific headquarters.<sup>295</sup> Coordinating US–Canada emergency plans to protect the flow of power to these installations could benefit the security of both nations.

The US–Canada Permanent Joint Board on Defense provides an ideal venue to explore such coordination options. Established in 1940 to discuss and advise on issues related to continental defense and security, the board has focused increasing attention on binational opportunities to strengthen critical infrastructure resilience. In 2011, the CEO of NERC led a

Permanent Joint Board on Defense discussion of how North American BPS emergency plans and coordination mechanisms could benefit US and Canadian national security. Natural Resources Canada and DOE have also participated in subsequent Permanent Joint Board on Defense meetings, along with the defense departments of both nations and critical infrastructure stakeholders. US and Canadian officials should consider using the board to facilitate industry–government discussions on opportunities to coordinate in grid security emergencies.

### **Coordination with Mexico and Beyond: Multinational Resilience against Grid Security Emergencies**

The US grid has much less connectivity with Mexican electric systems than with the Canadian grid. Southern California and a portion of Mexico’s Baja California have synchronous interconnections. Along the Mexico–Texas border, asynchronous interconnections also exist between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities.<sup>296</sup> In 2017, Mexican and US officials agreed to nonbinding pledges to increase this connectivity in ways that would strengthen reliability on both sides of the border.<sup>297</sup>

The election of Mexican president Andrés Manuel López Obrador in July 2018 may lead to significant changes in that country’s energy policies.<sup>298</sup> Structural challenges will also slow efforts to increase US–Mexico grid integration, including repeated power shortages and major shortfalls in the functionality of the Mexican grid.<sup>299</sup> Nevertheless, it could be useful to expand discussions with industry and the incoming government on protecting grid reliability against cyber and physical threats.

<sup>293</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 12.

<sup>294</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 11.

<sup>295</sup> “Maritime Forces Pacific,” Royal Canadian Navy.

<sup>296</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–4.

<sup>297</sup> “Increasing Electricity Cooperation in North America,” DOE.

<sup>298</sup> Kissane and Medina, “Energy Aftershocks.”

<sup>299</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–13.

Building grid security emergency coordination mechanisms beyond North America would also be helpful. As noted earlier, attacks on the US grid are most likely to occur in the context of an intense, escalating regional crisis in the Baltics, Northeast Asia, or some other area where US allies and critical security interests are at risk. In particular, adversaries may seek to inflict blackouts that could disrupt the deployment of US forces to the crisis zone. But we should also expect that US allies in the region will suffer attacks on their own grids, aimed at disrupting their ability to conduct combined operations with the United States and deliver electricity to US bases on their territories.

NATO's 2018 Locked Shields exercise focused on building alliance-wide preparedness for cyber and physical attacks against energy and communications systems.<sup>300</sup> In future exercises, allies might explore how to jointly determine whether grid attacks are potentially imminent and coordinate on the implementation of conservative operations across NATO member countries. The United States might explore equivalent opportunities for collaboration with Japan, South Korea, Australia, New Zealand, and other security partners. Existing treaty commitments, including those under Article V of NATO's founding treaty, will provide a starting point to meet our shared grid resilience challenges.<sup>301</sup>

### Playing Defense in Cyberwarfare: Doctrine, Integrated Planning, and Benefits for Deterrence

Utility leaders are urging the federal government to do more to assist them in deterring and defeating attacks on the grid. Their calls come at a perfect time. Administration officials have opened the door to new forms of operational collaboration between industry and government, including "collective

defense" during cyber attacks.<sup>302</sup> This report examines an especially significant option to expand their collaboration: coordinating the implementation of emergency orders with DOD operations to halt attacks at their source.

Deeper operational partnerships can also help meet underlying challenges for cyber deterrence. A number of cybersecurity analysts argue that deterrence by denial is impractical in cyberspace because offensive cyber capabilities are so much stronger than cyber defenses, and because cyber warfare will be very different from conventional conflicts. Analysts also warn that the United States lives in a cyber "glass house": given the vulnerability of the power grid and other infrastructure systems, the president cannot credibly threaten to use cyber weapons to defend US allies and interests. Improving preparedness for grid security emergencies can help address these concerns and support ongoing reassessments of US strategies for deterrence.

### Unity of Effort in Defensive Operations at Home and Abroad

Tom Fanning, CEO of Southern Company (one of the largest power companies in the United States), notes that he and other infrastructure owners and operators face a major constraint on their ability to defend their systems: "I can't fight back."<sup>303</sup> In theory, blunting attacks at their source could greatly ease the scale and severity of the threats that utilities will need to counter. In practice, integrating grid security emergency operations with measures to suppress enemy attacks would entail major policy and technical obstacles.

Power companies should not be responsible for striking enemies' offensive cyber infrastructure during grid security emergencies. The US government is the sole actor with the prerogative to engage in techniques such as "hacking back" that

<sup>300</sup> Cowan, "Locked Shields 2018."

<sup>301</sup> "The North Atlantic Treaty," NATO.

<sup>302</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>303</sup> Smith, "U.S. Officials Push New Penalties."

involve operations to disrupt or destroy an attacker's system.<sup>304</sup> Moreover, even if power companies gained legal authority to fight back against adversaries, their technical capacity to do so would be dwarfed by the capabilities possessed by US Cyber Command and other US government organizations.

Efforts to integrate defensive operations at home and abroad should rest on the comparative advantages of industry and government. BPS entities and other components of the electricity subsector are best positioned to defend their systems from within, assisted by DOE and other government partners. Operations abroad to halt attacks on the grid should remain the exclusive purview of government agencies, supported by industry assistance to gather malware samples and facilitate attack attribution. Based on this division of labor, government and industry leaders could explore whether and how to strengthen unity of effort for the full scope of defensive operations within the United States and beyond.

Secretary of homeland security Kirstjen Nielsen has called for the adoption of a "collective defense" posture that might include such expanded partnerships. Under the collective defense model, industry and government would collaborate to act on threat indicators and "respond more quickly and effectively to incidents."<sup>305</sup> The most familiar realm of operational collaboration lies in government support to help utilities detect, characterize, and eradicate malware on their systems. DHS is strengthening the National Cybersecurity and Communications Integration Center's ability to provide such assistance.<sup>306</sup> State National Guard organizations can also support post-cyber attack power restoration within the larger context of the industry's Cyber Mutual Assistance system.<sup>307</sup> However, in a cyber strike against the

United States, DOD will require many of these same guard personnel to protect the department's networks, conduct cyber operations against the attacker, and carry out other federal missions.<sup>308</sup> Power companies and government agencies will need to continue clarifying whether and how specific National Guard assets can help meet utility requests for assistance; existing doctrine and procedures for providing defense support to civil authorities offer a solid basis to advance those discussions.

In contrast, coordinating industry grid protection measures with government operations to suppress attacks would extend collective defense into uncharted territory. The command vision for US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, offers a starting point to examine how engaging against malicious cyber actors might help protect utilities. The document states that the United States must "increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage." To do so, DOD "is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems."<sup>309</sup>

Forward defense operations could respond to and help counter adversary efforts to implant malware on utility networks. Should such operations also help power companies protect their systems if the president declares that an attack is imminent? As senator Mike Rounds frames the question: "If someone is going to shoot an arrow at you, do you shoot the archer before he shoots the arrow?"<sup>310</sup>

US Cyber Command's vision statement does not directly address this possibility. However, each phase of grid security emergencies will likely offer

<sup>304</sup> GWU, *Into the Gray Zone*, 25.

<sup>305</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>306</sup> Marks, "DHS Stands Up New Cyber Risk Center."

<sup>307</sup> Crowe, "National Guard Preparing"; and Puryear, "91st Cyber Brigade Activated."

<sup>308</sup> DOD, *Cyber Strategy*, 4.

<sup>309</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 4–5.

<sup>310</sup> Bordelon, "Rounds Is Ready."



a different mix of risks and rewards for combining domestic and forward defense operations. For example, if the president determines that an attack on the grid is imminent, the secretary might issue orders for conservative operations to bolster grid defenses at the same moment that forward defense operations disrupted enemy cyber infrastructure poised to launch the strike. But assessments that an attack is imminent may turn out to be wrong. No-regrets orders for conservative operations are valuable precisely because using them will entail few consequences if warning indicators turn out to be false. Preattack forward defense operations could start a cyberwar that might not otherwise have occurred.

The United States can avoid such risks by waiting until attacks on the grid are under way before striking the enemy's offensive infrastructure. However, developing the technical capabilities to identify and disrupt the cyber infrastructure being used in an attack could prove challenging. Moreover, it is not clear whether integrating plans for home and away operations would offer significant benefits, as opposed to relying on utilities and government agencies to conduct those two types of operations independently.

US Cyber Command has opened the door to building new types of partnerships with the electricity subsector. The command has called for measures to "deepen and operationalize" collaboration between the private sector, the armed services, and other command partners.<sup>311</sup> As those efforts go forward with the electricity subsector and DOE, exploring options for collective defense (and clarifying the dangers they might present) should be a prime focus for analysis.

### **Maximizing Industry Contributions to Cyber Deterrence by Denial**

The *National Security Strategy* emphasizes that rather than rely on threats of cost imposition alone

to deter enemy attacks, the United States will also strengthen deterrence by denial. This report has examined how grid security emergency orders and implementation plans can raise adversaries' doubts as to whether they can achieve their objectives. But strengthening this form of deterrence will also entail underlying challenges.

Many cybersecurity analysts believe that offensive cyber capabilities are vastly stronger than defenses against them, and that this preeminence creates destabilizing incentives for adversaries to strike first when conflicts loom.<sup>312</sup> Unless measures to strengthen grid resilience can help weaken the dominance of offense over defense in the cyber realm, deterrence by denial will remain difficult to accomplish against highly capable adversaries.

However, today's offensive dominance stems in part from historical factors that are rapidly changing. The interconnected grid evolved decades ago when no cyber threat existed to drive protective measures. Moreover, as utilities began incorporating computer-assisted controls, sensors, and operating technology systems, few of these companies accounted for the risk that cyber threats to their systems would escalate so rapidly. As noted in this report, utilities are advancing a wide array of technical initiatives and fallback operational plans to counter and (ideally) stay ahead of adversaries' capabilities. In addition, regulatory bodies across the nation are increasingly willing to enable companies to recover costs for cyber resilience.

The current preeminence of offense over defense also reflects organizational factors. Rebecca Slayton has found that historically, "the success of offense is largely the result of a poorly managed defense."<sup>313</sup> The skills of the individuals employing cyber weapons and defensive tools, and the effectiveness with which

---

<sup>311</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 8.

---

<sup>312</sup> For a review of this "offense-dominant" literature, and the smaller set of works opposing it, see Slayton, "What Is the Cyber Offense-Defense Balance?," 72.

<sup>313</sup> Slayton, "What Is the Cyber Offense-Defense Balance?," 87.



these practitioners are managed and organized, have an enormous impact on the outcome of cyber engagements. Slayton notes that the importance of organization for cyber defense is implicit in discussions of the need for better public-private partnerships and information sharing. What has been missing, however, are efforts to make such partnerships *operational* and create unity of effort in government-industry defense actions when adversaries strike. That is precisely the gap that DOE and its industry partners can fill by developing grid security emergency orders and advancing all of the other collaborative initiatives necessary to make those orders effective.

Improved partnerships and technical capabilities to protect the grid cannot by themselves make defense preeminent. To further rebalance offense and defense in cyberspace, resilience initiatives will be necessary across all critical infrastructure sectors, as well as a host of other measures to facilitate the command, control, and coordination of public-private defensive operations. But building preparedness for grid security emergencies will be vital for that broader effort. Moreover, establishing defensive primacy is not necessary to facilitate deterrence by denial. As defined by the *National Security Strategy*, deterrence by denial functions by creating doubt in our adversaries that they can achieve their objectives.<sup>314</sup> DOE and its partners should develop grid security emergency orders that (perhaps in conjunction with forward defense operations) can make adversaries less likely to attack, even if defensive dominance remains out of reach.

Strengthening grid resilience can also support the broader reassessment of the US deterrence posture that is now under way. Robert Strayer, the State Department's deputy assistant secretary for cyber and international communications and information policy, notes that the increasing severity of threats to

US infrastructure is forcing "an evolution in the US government's thinking about how to deter malicious cyber actors."<sup>315</sup> In conventional warfare, deterrence by denial functions by making it physically difficult for adversaries to achieve their objectives and by raising enemy forces' costs of taking their targets.<sup>316</sup> Cyberwarfare will not entail the same sorts of attrition of enemy forces that occurs in battles with tanks, fighter aircraft, and other conventional weapons. The Trump and Obama administrations have redefined deterrence by denial to better fit the characteristics of cyberspace. The unique features of cyber conflict will require continued rethinking of how the United States can strengthen deterrence in the years to come. As utilities and government agencies build resilience for grid security emergencies, new opportunities will emerge to influence adversaries' perceived costs and benefits of attack. The United States should continue to refine its deterrence posture to capitalize on these improvements.

### Escaping the "Glass House" Syndrome

The president may need the ability to use cyber weapons against foreign targets to help resolve crises on terms favorable to the United States. The *DOD Cyber Strategy* (April 2015) states that:

There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an

<sup>314</sup> White House, *National Security Strategy*, 13.

<sup>315</sup> Smith, "U.S. Officials Push New Penalties."

<sup>316</sup> For definitions of classic deterrence by denial derived from conventional warfare, see Gerson, "Conventional Deterrence"; and Mitchell, "The Case for Deterrence by Denial." For an analysis of how that definition differs from that used by the Trump administration, see Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy."

ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests.<sup>317</sup>

However, any such operations against an adversary's cyber infrastructure would risk retaliatory strikes against the United States—including, potentially, attacks on the grid. Senator Thom Tillis (R-NC), a member of the Senate Armed Service Committee, emphasizes that the United States is living in “a big glass house.”<sup>318</sup> If US infrastructure owners and operators cannot defend their systems against attack, the president may be reluctant to use cyber weapons abroad, even if doing so might otherwise offer enormous benefits for conflict termination. In short: US leaders may be self-deterred from taking actions that they may need to employ. Developing emergency orders and implementation plans to protect grid reliability could reduce these glass house constraints and widen the range of options available for the president to protect US interests.

Improving grid defenses could also help strengthen the credibility of US commitments to defend key allies. Former US defense and intelligence officials have proposed that the United States and other high-cyber-capability NATO allies provide extended deterrence against cyber attacks for less capable alliance members.<sup>319</sup> But glass house concerns would call into question the credibility such commitments. Measures to strengthen grid resilience could help convince adversaries that the United States is willing to help allies respond to cyber attacks on their infrastructure.

Yet, nothing requires the United States to respond to such attacks with cyber weapons alone. On the contrary: the *National Security Strategy* and other policy documents leave open the possibility that

if cyber attacks at home or abroad are sufficiently severe, the United States will respond with conventional or even nuclear weapons. James Lewis notes that “opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return,” and will surely weigh that risk given “the immense capacity of the United States to inflict punishment” on attackers.<sup>320</sup> Emergency orders to protect the flow of power to defense installations can and should reinforce the certainty of that punishment.

But any first use of cyber weapons by the United States would entail escalatory dangers as well. If the United States were to initiate the use of destructive cyber weapons to defend US allies and interests, potential adversaries such as Russia could respond with conventional or nuclear forces. Moreover, conflicts that begin with the large-scale use of cyber weapons could also spiral out of control in ways that neither side desires or anticipates.<sup>321</sup> These escalatory risks must be in the forefront of calculations on whether and how to engage in cyber warfare. Indeed, as government agencies partner with power companies to build resilience for grid security emergencies, deterring such conflicts and reducing the likelihood of cyberwarfare should always be our prime objective.

<sup>317</sup> DOD, *Cyber Strategy*, 5.

<sup>318</sup> Schwartz, “Sen. Tillis: We Are Living in a Glass House.” For additional analysis of the glass house syndrome and its effects on constraining US options, see Miller, “Cyber Deterrence”; and Rosenbach, “Living in a Glass House.”

<sup>319</sup> Kramer, Butler, and Lotrionte, *Cyber, Extended Deterrence, and NATO*, 1.

<sup>320</sup> Lewis, *Rethinking Cybersecurity*, 9, 29. The author also argues that even if attacks on the grid occur, they would be unlikely to achieve the strategic effects that adversaries will seek, further reducing the likelihood of such attacks (see pp. 21 and 24–26).

<sup>321</sup> Danzig, *Surviving on a Diet of Poisoned Fruit*, 25; Lin, “Escalation Dynamics,” 52; and Miller and Fontaine, *A New Era*, 18–20.

## Bibliography

- 6 U.S.C. § 124l. <https://www.law.cornell.edu/uscode/text/6/124l>.
- 15 U.S.C. § 3361. <https://www.law.cornell.edu/uscode/text/15/3361>.
- 15 U.S.C. § 3363. <https://www.law.cornell.edu/uscode/text/15/3363>.
- 15 U.S.C. § 3364. <https://www.law.cornell.edu/uscode/text/15/3364>.
- 16 U.S.C. § 824a. <https://www.law.cornell.edu/uscode/text/16/824a>.
- 16 U.S.C. § 824o. <https://www.law.cornell.edu/uscode/text/16/824o>.
- 16 U.S.C. § 824o–1. [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).
- 18 CFR 388.113. <https://www.law.cornell.edu/cfr/text/18/388.113>.
- 47 U.S.C. § 606. <https://www.law.cornell.edu/uscode/text/47/606>.
- 50 U.S.C. Appendix §2071(c). <https://law.justia.com/codes/us/2001/title50/app/defensepr/sec2071/>.
- “About Alerts.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx>.
- “About NERC.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/AboutNERC/Pages/default.aspx>.
- “About NSTAC.” DOS (US Department of State). Last published June 20, 2016. <https://www.dhs.gov/about-nstac>.
- “About 60% of the U.S. Electric Power Supply Is Managed by RTOs.” US Energy Information Administration. April 4, 2011. <https://www.eia.gov/todayinenergy/detail.php?id=790>.
- “Alert (ICS-ALERT-14-281-01E): Ongoing Sophisticated Malware Campaign Compromising ICS (Update E).” ICS-CERT. Originally released December 10, 2014, last revised December 9, 2016. <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.
- “Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure.” ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). February 25, 2016. <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.
- “Alert (TA17-163A): CrashOverride Malware.” US-CERT (US Computer Emergency Readiness Team). June 12, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-163A>.
- “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). October 20, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-293A>.
- “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). March 15, 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.

- ASD(EI&E) (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment). *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*. Washington, DC: DOD, July 2017. <https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf>.
- Assante, Michael, and Robert M. Lee. *The Industrial Control System Cyber Kill Chain*. Bethesda, MD: SANS Institute, October 2015. <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.
- “Automated Indicator Sharing (AIS).” US-CERT (US Computer Emergency Readiness Team). n.d. <https://www.us-cert.gov/ais>.
- Banham, Russ. “DDoS Attacks Evolve to Conscript Devices onto the IoT.” *Forbes*, February 4, 2018. <https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#4b5a43a86aaa>.
- Barnes, Julian E. “‘Warning Lights Are Blinking Red,’ Top Intelligence Officer Says of Russian Attacks.” *New York Times*, July 13, 2018. <https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html>.
- Blue Ribbon Study Panel on Biodefense (Hudson Institute). *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts—A Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*. Washington, DC: Hudson Institute, October 2015. <http://www.biodefensestudy.org/a-national-blueprint-for-biodefense>.
- Bordelon, Brendan. “Rounds Is Ready to Lead New Senate Cybersecurity Subcommittee.” *Morning Consult*, February 1, 2017. <https://morningconsult.com/2017/02/01/rounds-ready-lead-new-senate-cybersecurity-subcommittee/>.
- Brown, Jared T., and Daniel H. Else. *The Defense Production Act of 1950: History, Authorities, and Reauthorization*. Washington, DC: Congressional Research Service, July 28, 2014. <https://fas.org/sgp/crs/natsec/R43118.pdf>.
- “The Canada-U.S. Defence Relationship.” Department of National Defence and the Canadian Armed Forces. December 4, 2014, last modified February 10, 2015. <http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s>.
- Cherepanov, Anton, and Robert Lipovsky. “Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet.” *WeLiveSecurity* (ESET Blog), June 12, 2017. <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.
- “Compendium of U.S.-Canada Emergency Management Assistance Mechanisms.” Public Safety Canada. October 2016, last modified March 28, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cmpndm-ntdstts-cnd-2016/index-en.aspx>.
- “Compliance - Québec.” Northeast Power Coordinating Council. n.d. <https://www.npcc.org/Compliance/Quebec/Forms/Public%20List.aspx>.
- Cowan, Gerrard. “Locked Shields 2018 Practises for Large-Scale Cyber Incident.” *Jane’s 360*, April 29, 2018. <http://www.janes.com/article/79652/locked-shields-2018-practises-for-large-scale-cyber-incident>.

- Crowe, Greg. "National Guard Preparing to Defend Cyberspace for States." *Federal News Radio*, April 16, 2018. <https://federalnewsradio.com/cyber-exposure/2018/04/national-guard-preparing-to-defend-cyberspace-for-states/>.
- "Cybersecurity." American Gas Association. n.d. <https://www.aga.org/safety/security/cybersecurity/>.
- "The Cyber Threat Framework." ODNI (Office of the Director of National Intelligence). n.d. <https://www.dni.gov/index.php/cyber-threat-framework>.
- Danzig, Richard. *Catastrophic Bioterrorism—What Is to Be Done?* Washington, DC: Center for Technology and National Security Policy, August 2003. [http://www.response-analytics.org/images/Danzig\\_Bioterror\\_Paper.pdf](http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf).
- . *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Washington, DC: Center for a New American Security, July 2014. [https://s3.amazonaws.com/files.cnas.org/documents/CNAS\\_PoisonedFruit\\_Danzig.pdf](https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf).
- Defense Science Board. *Task Force on Cyber Deterrence*. Washington, DC: DOD, February 2017. [https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport\\_02-28-17\\_Final.pdf](https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf).
- DHS (US Department of Homeland Security). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: DHS, December 17, 2003. <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- . *National Cyber Incident Response Plan*. Washington, DC: DHS, December 2016. [https://www.us-cert.gov/sites/default/files/ncirp/National\\_Cyber\\_Incident\\_Response\\_Plan.pdf](https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf).
- . *National Response Framework*. 3rd ed. Washington, DC: DHS, June 2016. [https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National\\_Response\\_Framework3rd.pdf](https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf).
- . *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS, 2013. <https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf>.
- . *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage*. Washington, DC: DHS, June 2017. <https://www.fema.gov/media-library/assets/documents/154058>.
- . *Strategy for Protecting and Preparing the Homeland against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*. Washington, DC: DHS, forthcoming.
- . *U.S. Department of Homeland Security Cybersecurity Strategy*. Washington, DC: DHS, May, 15, 2018. [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf).
- DiSavino, Scott, and David Sheppard. "ConEd Cuts Power to Part of Lower Manhattan Due to Sandy." *Reuters*, October 29, 2012. <https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030>.



- DOD (US Department of Defense). *Department of Defense Manual 3020.45*. Washington, DC: DOD, last updated May 23, 2017. <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>.
- . *DoD Cybersecurity Discipline Implementation Plan*. Washington, DC: DOD, amended February 2016. <http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf>.
- . *DOD Cyber Strategy*. Washington, DC: DOD, April 2015. [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).
- . *DoD Directive 3020.40: Mission Assurance (MA)*. Washington, DC: DOD, November 29, 2016. [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).
- . *Mission Assurance Strategy*. Washington, DC: DOD, April 2012. [http://policy.defense.gov/Portals/11/Documents/MA\\_Strategy\\_Final\\_7May12.pdf](http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf).
- DOE (US Department of Energy). “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40).” *Federal Register* 83, no. 7 (2018): 1176. <https://www.federalregister.gov/documents/2018/01/10/2018-00259/grid-security-emergency-orders-procedures-for-issuance>.
- . *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. Version 1.1. Washington, DC: DOE, February 2014. <https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf>.
- . *Electromagnetic Pulse Resilience Action Plan*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf>.
- . “Energy Priorities and Allocations System Regulations (RIN 1901–AB28).” *Federal Register* 76, no. 111 (2011): 33615. <https://www.gpo.gov/fdsys/pkg/FR-2011-06-09/pdf/2011-14282.pdf>.
- . *Multiyear Plan for Energy Sector Cybersecurity*. Washington, DC: DOE, March 2018. [https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20\\_0.pdf](https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf).
- . *Quadrennial Energy Review—Transforming the Nation’s Electricity System: The Second Installment of the QER*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>.
- . *Staff Report to the Secretary on Electricity Markets and Reliability*. Washington, DC: DOE, August 2017. [https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability\\_0.pdf](https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability_0.pdf).
- . *Strategic Transformer Reserve: Report to Congress*. Washington, DC: DOE, March 2017. <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.
- “DOE’s Use of Federal Power Act Emergency Authority.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use>.

- DOS (US Department of State). *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. Washington, DC: DOS, May 31, 2018. <https://www.state.gov/documents/organization/282253.pdf>.
- Dougherty, Jon. “Biggest U.S. Power Grid Operator Suffers Thousands of Attempted Cyber Attacks per Month.” *Forward Observer*, August 28, 2017. <https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/>.
- Douris, Constance. “DARPA Research Leads Grid Security Solutions.” *The Buzz* (blog), *National Interest*, January 12, 2017. <http://nationalinterest.org/blog/the-buzz/darpa-research-leads-grid-security-solutions-19044>.
- Dragos, Inc. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. Hanover, MD: Dragos, June 13, 2017. <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>.
- EEL (Edison Electric Institute). “Comments of the Edison Electric Institute.” In *Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*. February 6, 2017.
- . *Understanding the Electric Power Industry’s Response and Restoration Process*. Washington, DC: EEL, October 2016. [http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA\\_101FINAL.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf).
- EIS Council (Electric Infrastructure Security Council). *E-PRO Handbook II: Volume 1—Fuel*. Washington, DC: EIS Council, 2016. [https://www.eiscouncil.org/App\\_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf](https://www.eiscouncil.org/App_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf).
- . *E-PRO Handbook III: Black Sky Cross-Sector Coordination and Communication*. Washington, DC: EIS Council, June 2018. [https://www.eiscouncil.org/EPRO\\_Books.aspx](https://www.eiscouncil.org/EPRO_Books.aspx).
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS-ICS. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Washington, DC: NERC, March 2016. [https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_18Mar2016.pdf](https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf).
- “Electricity Information Sharing and Analysis Center.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.
- “Electric Power Transmission Reliability Standards Compliance Monitoring and Enforcement.” Régie de l’énergie Québec. n.d. <http://www.regie-energie.qc.ca/en/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html>.
- “Emergency Communications.” DHS (US Department of Homeland Security). Last published June 26, 2018. <https://www.dhs.gov/topic/emergency-communications>.
- Energy Policy Act of 2005. Public Law 109-58. *U.S. Statutes at Large* 119 (2005): 942–943. <https://www.gpo.gov/fdsys/pkg/STATUTE-119/pdf/STATUTE-119.pdf>.
- “Energy Sector Cybersecurity Preparedness.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

- EPRI (Electric Power Research Institute). *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research*. Report 3002000796. Palo Alto, CA: EPRI, December 2013. <https://publicdownload.epri.com/PublicDownload.svc/product=000000003002000796/type=Product>.
- . *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs*. Report 3002008999. Palo Alto, CA: EPRI, September 2016. <https://www.epri.com/#/pages/product/000000003002008999/?lang=en>.
- ESCC (Electricity Subsector Coordinating Council). *Electricity Sub-Sector Coordinating Council Charter*. Washington, DC: DHS, August 5, 2013. <https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf>.
- “ESCC: Electricity Subsector Coordinating Council.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.
- “The ESCC’s Cyber Mutual Assistance Program.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1>.
- FEMA (US Federal Emergency Management Agency). *2017 Hurricane Season FEMA After-Action Report*. Washington, DC: FEMA, July 12, 2018. <https://www.fema.gov/media-library/assets/documents/167249>.
- FERC (Federal Energy Regulatory Commission). *Cyber Security Incident Reporting Reliability Standards*. 161 FERC ¶ 61,291. December 21, 2017. <https://www.ferc.gov/whats-new/comm-meet/2017/122117/E-1.pdf>.
- . *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies, Statement of Policy*. 96 FERC ¶ 61,299. September 14, 2011.
- . *Grid Resilience in Regional Transmission Organizations and Independent System Operators*. 162 FERC ¶ 61,256. 2018. <https://www.ferc.gov/CalendarFiles/20180320102618-AD18-7-000.pdf>.
- . *Order Authorizing Acquisition and Disposition of Jurisdictional Facilities*. 163 FERC ¶ 61,005. April 3, 2018. <https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf>.
- . *Order Granting Approvals in Connection with the Dissolution of the Southwest Power Pool Regional Entity*. 163 FERC ¶ 61,094. May 4, 2018. <https://www.ferc.gov/CalendarFiles/20180504141902-RR18-3-000.pdf>.
- . *Policy Statement on Matters Related to Bulk Power System Reliability*. 107 FERC ¶ 61,052. April 19, 2004. <https://www.ferc.gov/whats-new/comm-meet/041404/E-6.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833. 157 FERC ¶ 61,123. November 17, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-4.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833-A. 163 FERC ¶ 61,125. May 17, 2018. <https://www.ferc.gov/whats-new/comm-meet/2018/051718/E-2.pdf>.

- . *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*. 156 FERC ¶ 61,215. September 22, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/092216/E-4.pdf>.
- . *Revision to Electric Reliability Organization Definition of Bulk Electric System*. Order No. 743. 133 FERC ¶ 61,150. November 18, 2010. <https://www.ferc.gov/whats-new/comm-meet/2010/111810/E-2.pdf>.
- . *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*. Order No. 773-A. 143 FERC ¶ 61,053. April 18, 2013. <https://www.ferc.gov/whats-new/comm-meet/2013/041813/E-9.pdf>.
- FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation). *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*. Washington, DC: FERC, January 2016. <https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Further Joint Study Report: Planning Restoration Absent SCADA or EMS (PRASE)*. Washington, DC: FERC, June 2017. <https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Recommended Study: Blackstart Resources Availability (BRAv)*. Washington, DC: FERC, May 2018. <https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf>.
- Fischerkeller, Michael P., and Richard J. Harknett. “Deterrence Is Not a Credible Strategy for Cyberspace.” *Orbis* 61, no. 3 (2017): 381–393. <https://www.sciencedirect.com/science/article/pii/S0030438717300431>.
- Fixing America’s Surface Transportation Act, Public Law 114-94. *U.S. Statutes at Large* 129 (2015): 1773–1774. <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.
- Frankel, Alison. “Can Customers Sue Power Companies for Outages? Yes, but It’s Hard to Win.” *Reuters* (blog), November 9, 2012. <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>.
- Galloway, T. J., Sr. “Advancing Reliability and Resilience of the Grid.” Comments presented at the FERC Reliability Technical Conference, Washington, DC, July 31, 2018. <https://www.ferc.gov/CalendarFiles/20180731084251-Galloway,%20North%20American%20Transmission%20Forum.pdf>.
- Gerson, Michael S. “Conventional Deterrence in the Second Nuclear Age.” *Parameters* 39 (Autumn 2009): 32–48. <https://ssi.armywarcollege.edu/pubs/parameters/articles/09autumn/gerson.pdf>.
- Governments of the US and Canada. *Joint United States-Canada Electric Grid Security and Resilience Strategy*. Washington, DC: The White House, December 2016. [https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint\\_US\\_Canada\\_Grid\\_Strategy\\_06Dec2016.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf).
- GWU (George Washington University) Center for Cyber and Homeland Security. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: GWU, October 2016. <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf>.
- Healy, Jason. *The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities*. SSRN, June 2016. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2836206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206).



- Homeland Security Advisory Council. *Final Report of the Cybersecurity Subcommittee: Part I—Incident Response*. Washington, DC: DOS, June 2016. <https://www.hsd.org/?view&did=794271>.
- ICF. *Assessment of Large Power Transformer Risk Mitigation Strategies*. Fairfax, VA: ICF, October 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf>.
- . *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. Fairfax, VA: ICF, June 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>.
- “Increasing Electricity Cooperation in North America.” DOE (US Department of Energy). January 11, 2017. <https://www.energy.gov/policy/articles/increasing-electricity-cooperation-north-america>.
- INL (Idaho National Laboratory). *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*. Idaho Falls, IN: INL, January 2016. <https://inldigitallibrary.inl.gov/sites/STI/STI/INL-EXT-15-35582.pdf>.
- ISO-NE (ISO New England). *Operational Fuel-Security Analysis*. Holyoke, MA: ISO-NE, January 17, 2018. [https://www.iso-ne.com/static-assets/documents/2018/01/20180117\\_operational\\_fuel-security\\_analysis.pdf](https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf).
- . “Response of ISO New England Inc.” *Response to Grid Resilience in Regional Transmission Organization and Independent System Operators* (AD18-7-000). March 9, 2018. [https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7\\_iso\\_response\\_to\\_grid\\_resilience.pdf](https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7_iso_response_to_grid_resilience.pdf).
- Jenkins, Brian Michael. “Countering al-Qaeda: The Next Phase in the War.” *The RAND Blog*, September 8, 2002. <https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html>.
- Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*. Joint Publication 1. Washington, DC: Joint Chiefs of Staff, July 12, 2017. [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1\\_ch1.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf).
- Joint Commenters. “Comments of American Public Power Association, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group.” In *Response to RIN 1901-AB40*. February 23, 2017. <http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf>.
- Kaften, Cheryl. “DoD Tests Energy Continuity with ‘Islanded’ Microgrid.” *Energy Manager Today*, April 5, 2017. <https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/>.
- Kappenman, John. *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*. Goleta, CA: Metatech, January 2010. [https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc\\_meta-r-319.pdf](https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf).
- “Key Players.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>.
- Kissane, Carolyn, and Emily Medina. “Energy Aftershocks in Store after Seismic Mexican Election.” *The Hill*, July 3, 2018. <http://thehill.com/opinion/energy-environment/395383-energy-aftershocks-in-store-after-seismic-mexican-election>.



- Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte. *Cyber, Extended Deterrence, and NATO*. Washington, DC: Atlantic Council, May 2016. [http://www.atlanticcouncil.org/images/publications/Cyber\\_Extended\\_Deterrence\\_and\\_NATO\\_web\\_0526.pdf](http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf).
- Lawrence, Bill, Charlotte de Seibert, and Philip Daigle. "E-ISAC Update." Presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, FL, March 6–7, 2018. <https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf>.
- Lazar, Jim. *Electricity Regulation in the US: A Guide*. 2nd ed. Montpelier, VT: Regulatory Assistance Project, June 2016. <http://www.raponline.org/wp-content/uploads/2016/07/rap-lazar-electricity-regulation-US-june-2016.pdf>.
- Lewis, James A. "North Korea and Cyber Catastrophe—Don't Hold Your Breath." *38 North*, January 12, 2018. <http://www.38north.org/2018/01/jalewis011218/>.
- . *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Washington, DC: CSIS, January 2018. [http://espas.eu/orbis/sites/default/files/generated/document/en/180108\\_Lewis\\_ReconsideringCybersecurity\\_Web.pdf](http://espas.eu/orbis/sites/default/files/generated/document/en/180108_Lewis_ReconsideringCybersecurity_Web.pdf).
- Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. [http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06\\_Issue-3/Fall12.pdf](http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-3/Fall12.pdf).
- Lucas, Todd. "Conservative Operations." Presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, CO, September 18–19, 2013. <http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf>.
- Lynch, Justin. "How the Russian Government Allegedly Attacks the American Electric Grid." *Fifth Domain*, July 24, 2018. <https://www.fifthdomain.com/critical-infrastructure/2018/07/24/how-the-russian-government-attacks-the-american-electric-grid/>.
- Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (Sept./Oct. 2010). <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.
- "Maritime Forces Pacific." Royal Canadian Navy. Last modified November 24, 2016. <http://www.navy-marine.forces.gc.ca/en/about/structure-marpac-home.page>.
- Marks, Joseph. "DHS Stands up New Cyber Risk Center to Protect High-Value Targets." *Nextgov*, July 31, 2018. <https://www.nextgov.com/cybersecurity/2018/07/dhs-stands-new-cyber-risk-center-protect-high-value-targets/150179/>.
- Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn. *Power Begins at Home: Assured Energy for U.S. Military Bases*. Reston, VA: Noblis, January 12, 2017. [http://www.pewtrusts.org/~media/assets/2017/01/ce\\_power\\_begins\\_at\\_home\\_assured\\_energy\\_for\\_us\\_military\\_bases.pdf](http://www.pewtrusts.org/~media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf).
- McElwee, Steven. "Probabilistic Cluster Ensemble Evaluation for Unsupervised Intrusion Detection." Unpublished thesis, Nova Southeastern University, forthcoming.

- McElwee, Steven, Jeffrey Heaton, James Fraley, and James Cannady. "Deep Learning for Prioritizing and Responding to Intrusion Detection Alerts." In *2017 IEEE Military Communications Conference Proceedings*. Piscataway, NJ: IEEE, 2017. <https://ieeexplore.ieee.org/document/8170757/>.
- McGhee, Michael. "EEI Executive Advisory Committee." Slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017. [http://www.asaie.army.mil/Public/ES/oei/docs/EEI\\_Exec-Committee.pdf](http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf).
- Miller, James N. "Cyber Deterrence Cannot Be One Size Fits All." *Cipher Brief*, August 3, 2017. [https://www.thecipherbrief.com/column\\_article/cyber-deterrence-cannot-be-one-size-fits-all-1092](https://www.thecipherbrief.com/column_article/cyber-deterrence-cannot-be-one-size-fits-all-1092).
- Miller, James N., and James R. Gosler. "Memorandum for the Chairman, Defense Science Board" (preamble). In *Task Force on Cyber Deterrence*. Washington, DC: Defense Science Board, February 2017. <http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>.
- Miller, James N., Jr., and Richard Fontaine. *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict*. Washington, DC: CNAS, September 2017. <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Project Pathways-Finalb.pdf?mtime=20170918101505>.
- Miller, Rich. "Con Edison Shuts off Power in Lower Manhattan." *DataCenter Knowledge*, October 29, 2012. <http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutdown>.
- MISO (Midcontinent Independent System Operator). *Geomagnetic Disturbance Operations Plan*. SO-P-AOP-01 Rev: 1. Carmel, IN: MISO, June 9, 2017. [https://old.misoenergy.org/\\_layouts/miso/ecm/redirect.aspx?id=252214](https://old.misoenergy.org/_layouts/miso/ecm/redirect.aspx?id=252214).
- . "MISO January 17–18 Maximum Generation Event Overview." Slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018. <https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf>.
- Mitchell, A. Weiss. "The Case for Deterrence by Denial." *American Interest*, August 12, 2015. <https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/>.
- "M-1 Reserve Margin." NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.
- Murauskaite, Egle. "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment." *38 North*, September 12, 2014. <http://www.38north.org/2014/09/emurauskaite091214/>.
- Nakashima, Ellen. "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks." *Washington Post*, July 8, 2017. [https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47\\_story.html](https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html).
- NARUC (National Association of Regulatory Utility Commissioners). *Cybersecurity: A Primer for State Utility Regulators*. Version 3.0. Washington, DC: NARUC, January 2017. <https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F>.

- . *Resolution on Physical Security*. Washington, DC: NARUC, July 16, 2014. <https://pubs.naruc.org/pub.cfm?id=53A0CAA5-2354-D714-5127-E0C411BAD460>.
- NASEO (National Association of State Energy Officials). “Comments of the National Association of State Energy Officials.” In *Response to RIN 1901–AB40*. [https://www.naseo.org/Data/Sites/1/naseo-comments\\_rin-1901%E2%80%93ab40.pdf](https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901%E2%80%93ab40.pdf).
- NATF (North American Transmission Forum). *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—A Spare Tire Approach*. Charlotte, NC: NATF, 2017. <http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf>.
- . *North American Transmission Forum External Newsletter*. Charlotte, NC: NATF, January 2018. <https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf>.
- National Defense Authorization Act for Fiscal Year 2017. Public Law 114-328. *U.S. Statutes at Large* 130 (2016): 2685–2687. <https://www.gpo.gov/fdsys/pkg/PLAW-114publ328/pdf/PLAW-114publ328.pdf>.
- NERC (North American Electric Reliability Corporation). *BAL-002-2(i)—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. Washington, DC: NERC, January 1, 2018. [https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2\(i\).pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2(i).pdf).
- . *CIP-014-2—Physical Security*. Washington, DC: NERC, October 2, 2015. <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.
- . *EOP-010-1—Geomagnetic Disturbance Operations*. Washington, DC: NERC, June 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States).
- . *EOP-011-1—Emergency Operations*. Washington, DC: NERC, April 1, 2017. [https://www.nerc.com/\\_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).
- . *Glossary of Terms Used in NERC Reliability Standards*. Washington, DC: NERC, last updated July 3, 2018. [https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary\\_of\\_Terms.pdf](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf).
- . *Grid Security Exercise: GridEx III Report*. Atlanta, GA: NERC, March 2016. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.
- . *Grid Security Exercise GridEx IV: Lessons Learned*. Atlanta, GA: NERC, March 28, 2018. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf>.
- . *History of NERC*. Washington, DC: NERC, August 2013. <http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf>.
- . *Hurricane Harvey Event Analysis Report*. Washington, DC: NERC, March 2018. [https://www.nerc.com/pa/rrm/ea/Hurricane\\_Harvey\\_EAR\\_DL/NERC\\_Hurricane\\_Harvey\\_EAR\\_20180309.pdf](https://www.nerc.com/pa/rrm/ea/Hurricane_Harvey_EAR_DL/NERC_Hurricane_Harvey_EAR_20180309.pdf).

- . “Informational Filing on the Definition of ‘Adequate Level of Reliability.’” Filing to the Federal Energy Regulatory Commission. May 10, 2013. [https://www.nerc.com/pa/Stand/Resources/Documents/Adequate\\_Level\\_of\\_Reliability\\_Definition\\_\(Informational\\_Filing\).pdf](https://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf).
- . *IRO-008-2—Reliability Coordinator Operational Analysis and Real-Time Assessments*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/IRO-008-2.pdf>.
- . *PRC-010-2—Under Voltage Load Shedding*. Washington, DC: NERC, April 2, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States).
- . *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*. Atlanta, GA: NERC, December 13, 2017. [https://www.nerc.com/comm/OC\\_Reliability\\_Guidelines\\_DL/Gas\\_and\\_Electrical\\_Operational\\_Coordination\\_Considerations\\_20171213.pdf](https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Gas_and_Electrical_Operational_Coordination_Considerations_20171213.pdf).
- . *Reliability Terminology*. Atlanta, GA: NERC, August 2013. <https://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf>.
- . *Short-Term Special Assessment: Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation*. Atlanta, GA: NERC, May 2016. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric\\_Final.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric_Final.pdf).
- . *Standard PRC-006-3—Automatic Underfrequency Load Shedding*. Washington, DC: NERC, October 1, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States).
- . *Technical Report Supporting Definition of Adequate Level of Reliability*. Washington, DC: NERC, March 26, 2013. <https://www.nerc.com/comm/Other/Pages/Adequate%20Level%20of%20Reliability%20Task%20Force%20ALRTF.aspx>.
- . *TOP-001-3—Transmission Operations*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-001-3.pdf>.
- . *TPL-007-1—Transmission System Planned Performance for Geomagnetic Disturbance Events*. Washington, DC: NERC, December 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States).
- . *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power Phase II: A Vulnerability and Scenario Assessment for the North American Bulk Power System*. Atlanta, GA: NERC, May 2013. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC\\_PhaseII\\_FINAL.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf).
- . *2016 Long-Term Reliability Assessment*. Atlanta, GA: NERC, December 2016. <https://www.nerc.com/pa/rapa/ra/reliability%20assessments%20dl/2016%20long-term%20reliability%20assessment.pdf>.
- . *VAR-001-4.2—Voltage and Reactive Control*. Washington, DC: NERC, September 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/VAR-001-4.2.pdf>.



- NERC (North American Electric Reliability Corporation) Steering Group. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* Princeton, NJ: NERC, July 13, 2014. [https://www.nerc.com/docs/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](https://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC (North American Electric Reliability Corporation) System Protection and Control Subcommittee. *Reliability Fundamentals of System Protection*. Princeton, NJ: NERC, December 2010. [https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals\\_Approved\\_20101208.pdf](https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals_Approved_20101208.pdf).
- NETL (National Energy Technology Laboratory). *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units—Volume I: The Critical Role of Thermal Units during Extreme Weather Events*. Washington, DC: DOE, March 13, 2018. <https://www.netl.doe.gov/research/energy-analysis/search-publications/vuedetails?id=2594>.
- Newman, Lily Hay. “Hacker Lexicon: What Is the Attribution Problem?” *Wired*, December 24, 2016. <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.
- NIAC (National Infrastructure Advisory Council). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. Washington, DC: NIAC, August 2017. <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>.
- Nielsen, Kirstjen M. “National Cybersecurity Summit Keynote Speech.” DHS (Department of Homeland Security). Released July 31, 2018. <https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech>.
- “NOAA Space Weather Scales.” NOAA. April 2011. <https://www.swpc.noaa.gov/sites/default/files/images/NOAAScales.pdf>.
- “North America.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/Canada.aspx>.
- “The North Atlantic Treaty.” North Atlantic Treaty Organization. April 4, 1949 (as amended). [https://www.nato.int/cps/ic/natohq/official\\_texts\\_17120.htm](https://www.nato.int/cps/ic/natohq/official_texts_17120.htm).
- Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016/2017): 44–71. [https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\\_a\\_00266](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266).
- Obama, Barack. *Executive Order—Assignment of National Security and Emergency Preparedness Communications Functions*. Washington, DC: The White House, July 6, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness->.
- . *Executive Order—Coordinating Efforts to Prepare the Nation for Space Weather Events*. Washington, DC: The White House, October 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events>.
- . *Executive Order—Improving Critical Infrastructure Cybersecurity*. Executive Order 13636. Washington, DC: The White House, February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

- . *Executive Order—National Defense Resources Preparedness*. Washington, DC: The White House, March 16, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/03/16/executive-order-national-defense-resources-preparedness>.
- . *United States Cyber Incident Coordination*. Presidential Policy Directive 41. Washington, DC: The White House, July 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
- ODNI (Office of the Director of National Intelligence). *A Common Threat Framework: A Foundation for Communication*. McLean, VA: ODNI, January 26, 2018.
- Orenstein, Daniel G., and Lexi C. White. *Emergency Declaration Authorities across All States and D.C.* Edina, MN: Network for Public Health Law, June 16, 2015. [https://www.networkforphl.org/\\_asset/gxrdwm/Emergency-Declaration-Authorities.pdf](https://www.networkforphl.org/_asset/gxrdwm/Emergency-Declaration-Authorities.pdf).
- Paradise, Theodore J., et al. “ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance—RIN 1901–AB40.” Email to Jeffrey Baumgartner, US Department of Energy, February 6, 2017. [http://www.isorto.org/Documents/Report/20170206\\_Final\\_IRC-DOE\\_NOPR\\_Comments\\_re\\_Grid\\_Security\\_Emergency.pdf](http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf).
- Parfomak, Paul W. *Pipelines: Securing the Veins of the American Economy, Testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*. Washington, DC: Congressional Research Service, April 19, 2016. <http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf>.
- Parfomak, Paul W., Richard J. Campbell, Robert Pirog, Michael Ratner, Phillip Brown, John Frittelli, and Marc Humphries. *Cross-Border Energy Trade in North America: Present and Potential*. Washington, DC: Congressional Research Service, January 30, 2017. <https://fas.org/sgp/crs/misc/R44747.pdf>.
- Perry, Richard (US secretary of energy). Letter to the Federal Energy Regulatory Commission. September 28, 2017. <https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf>.
- Phillips, Tony. “Solar Shield—Protecting the North American Power Grid.” *NASA Science*, October 26, 2010. [https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\\_solarshield](https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield).
- PJM. “Comments and Responses of PJM Interconnection, L.L.C.” In *Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000). March 9, 2018. <http://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx>.
- . “Conservative Operations.” Training materials presented on January 27, 2015. <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.
- . *PJM Manual 13: Emergency Operations*. Rev. 65. Audubon, PA: PJM, January 1, 2018. <http://www.pjm.com/~/-/media/documents/manuals/m13.ashx>.

- Puryear, Cotton. "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade." *National Guard*, September 19, 2017. <http://www.nationalguard.mil/News/Article/1315685/91st-cyber-brigade-activated-as-army-national-guards-first-cyber-brigade/>.
- Reagan, Ronald. "The President's News Conference." August 12, 1986. Transcript. The American Presidency Project, Gerhard Peters and John T. Woolley. <http://www.presidency.ucsb.edu/ws/?pid=37733>.
- "Reliability Coordinators." NERC (North American Electric Reliability Corporation). As of June 1, 2015. <https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.
- "REMEDYS: Research Exploring Malware in Energy Delivery Systems." Cyber Resilient Energy Delivery Consortium. March 26, 2018. <https://cred-c.org/researchactivity/remedys-research-exploring-malware-energy-delivery-systems>.
- "The Role of Microgrids in Helping to Advance the Nation's Energy System." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/role-microgrids-helping>.
- "Roles and Responsibilities of Governments in Natural Resources." Natural Resources Canada. Last modified October 2, 2017. <http://www.nrcan.gc.ca/mining-materials/taxation/8882>.
- Rosenbach, Eric. "Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks." *Prepared Statement for the United States Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*. June 12, 2017. [https://www.foreign.senate.gov/imo/media/doc/061317\\_Rosenbach\\_Testimony.pdf](https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf).
- "Sandia's Grid Modernization Program Newsletter." Sandia National Laboratories. December 2017. <https://content.govdelivery.com/accounts/USDOESNLEC/bulletins/1c11ce6>.
- Schwartz, Ian. "Sen. Tillis: We Are Living in a Glass House Throwing Rocks Complaining about Election Interference." *RealClear Politics*, January 5, 2017. [https://www.realclearpolitics.com/video/2017/01/05/sen\\_tillis\\_we\\_are\\_living\\_in\\_a\\_glass\\_house\\_throwing\\_rocks\\_complaining\\_about\\_election\\_interference.html](https://www.realclearpolitics.com/video/2017/01/05/sen_tillis_we_are_living_in_a_glass_house_throwing_rocks_complaining_about_election_interference.html).
- "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response." DOE (Department of Energy). February 14, 2018. <https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency>.
- SERC. *Conservative Operations Guidelines*. Guide-800-101. Charlotte, NC: SERC, May 20, 2015. [https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines\\_rev-0-\(05-20-15\).pdf?sfvrsn=2](https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2).
- Severe Impact Resilience Task Force. *Severe Impact Resilience: Considerations and Recommendations*. Washington, DC: NERC, May 9, 2012. [https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF\\_Final\\_May\\_9\\_2012-Board\\_Accepted.pdf](https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf).

- Shelton, William L. "Threats to Space Assets and Implications for Homeland Security." *Written Testimony before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*. March 29, 2017. <http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf>.
- Sistrunk, Chris. "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)." *SANS Industrial Control Systems Security Blog*, January 8, 2016. <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>.
- Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (Winter 2016/17): 73–109. [https://www.mitpressjournals.org/doi/10.1162/ISEC\\_a\\_00267](https://www.mitpressjournals.org/doi/10.1162/ISEC_a_00267).
- Smith, Rebecca. "U.S. Officials Push New Penalties for Hackers of Electrical Grid." *Wall Street Journal*, August 5, 2018. <https://www.wsj.com/articles/u-s-officials-push-new-penalties-for-hackers-of-electrical-grid-1533492714>.
- Smith, Scott S. "Roles and Responsibilities for Defending the Nation from Cyber Attack." *Testimony Before the Senate Armed Services Committee*. October 19, 2017. <https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities>.
- Sobczak, Blake, Hannah Northey, and Peter Behr. "Cyber Raises Threat against America's Energy Backbone." *Energy Wire*, May 23, 2017. <https://www.eenews.net/stories/1060054924/>.
- Social Media Working Group for Emergency Services and Disaster Management. *Countering False Information on Social Media in Disasters and Emergencies*. Washington, DC: DHS, March 2018. [https://www.dhs.gov/sites/default/files/publications/SMWG\\_Countering-False-Info-Social-Media-Disasters-Emergencies\\_Mar2018-508.pdf](https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf).
- "Spare Transformers." EEI (Edison Electric Institute). n.d. <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.
- Stanley, Andrew J. *Mapping the U.S.-Canada Energy Relationship*. Washington, DC: CSIS, May 2018. [https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507\\_Stanley\\_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507_Stanley_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz).
- "State and Local Energy Assurance Planning." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/energy-assurance/emergency-preparedness/state-and-local-energy-assurance-planning>.
- State of New Jersey Board of Public Utilities. *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196). March 18, 2016. <http://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf>.
- Stockton, Paul. On behalf of Exelon Corporation. *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*. Docket No. RM18-1-000. October 23, 2017.
- . "Thresholds and Criteria for Declaring Grid Security Emergencies." Study for the US Department of Energy. January 31, 2018.



- Sukumar, Arun M. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare* (blog), July 4, 2017. <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.
- "Transmission Equipment Ready When Needed." Grid Assurance. n.d. <http://www.gridassurance.com/equipment-subscribers/>.
- Trump, Donald. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Executive Order 13800. Washington, DC: The White House, May 11, 2017. <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
- Ucci, Daniele, Leonardo Aniello, and Roberto Baldoni. "Survey on the Usage of Machine Learning Techniques for Malware Analysis." *ACM Transactions on the Web* 1, no. 1 (October 2017): 1:1–1:34. <https://pdfs.semanticscholar.org/d310/47e426b8b5c2aa52108899a800bedd966f07.pdf>.
- "United States Mandatory Standards Subject to Enforcement." NERC. n.d. <https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States>.
- U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington, DC: DOE, April 2004. <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.
- US Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington, DC: US Cyber Command, released March 2018. <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>.
- Van Broekhoven, S. B., N. Judson, S. V. T. Nguyen, and W. D. Ross. *Microgrid Study: Energy Security for DoD Installations*. Technical Report 1164. Lexington, MA: MIT, June 2012. <https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf>.
- Vine, Doug. *Interconnected: Canadian and U.S. Electricity*. Arlington, VA: Center for Climate and Energy Solutions, March 2017. <https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf>.
- Walker, Bruce J. *Written Testimony before the U.S. Senate Committee on Energy and Natural Resources*. March 1, 2018. [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=1C574731-A9C0-4E1C-9E05-15C492E332B1](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1).
- Weiss, Walter. "Rapid Attack Detection, Isolation and Characterization Systems (RADICS)." Defense Advanced Research Projects Agency. n.d. <https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems>.
- Western Electricity Coordinating Council. "Conservative System Operations." Training slides. n.d. <http://docplayer.net/55224883-Conservative-system-operations.html>.
- The White House. *National Security Strategy of the United States of America*. Washington, DC: The White House, December 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- "Work Continues on ITC Lake Erie Project." *Transmission Hub*, February 19, 2018. <https://www.transmissionhub.com/articles/2018/02/work-continues-on-itc-lake-erie-project.html>.



## Acknowledgments

My special thanks go to Robert Denaburg, senior analyst at Sonecon LLC. I also thank the following colleagues for helpful reviews of this study: Michael Assante (SANS Institute); Wayne Austad (Idaho National Laboratory); Terry Boston; Stuart Brindley; Gerry Cauley; Richard Danzig (JHU/APL); Daniel Elmore (Idaho National Laboratory); Peter Grandgeorge (Berkshire Hathaway Energy); Emily Goldman (US Cyber Command); Sean Griffin (ecubed us LLC); Dave Halla (JHU/APL); Jon Jipping (ITC Holdings); Debra Lavoy (Narrative Builders); Bill Lawrence (NERC); Joseph Maurio (JHU/APL); James Miller (JHU/APL); Michael Moskowitz (JHU/APL); Richard Mroz; Steven T. Naumann (Exelon Corporation); Catherine Peacock (JHU/APL); Emilia Probasco (JHU/APL); Erin Richardson (JHU/APL); David Roop (Dominion Energy); Matthew Schaffer (JHU/APL); senior leaders at Southern Company; Kyle Thomas (Dominion Virginia Power); and Virginia Wright (Idaho National Laboratory). I also thank the many additional industry and government reviewers who preferred to remain anonymous.

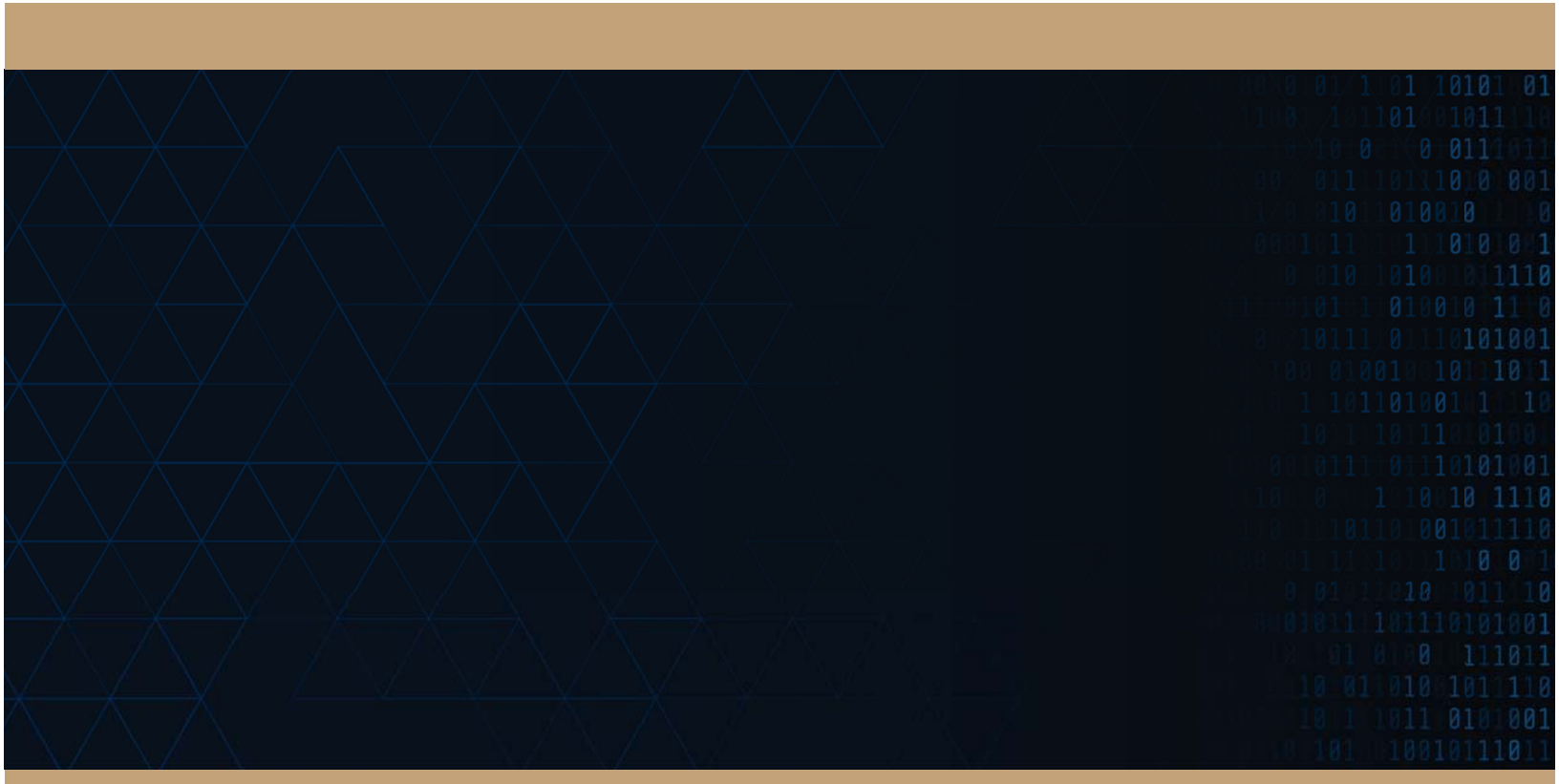
## About the Author

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC, and a senior fellow of JHU/APL. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support in Superstorm Sandy and other disasters. Dr. Stockton also served as the Department of Defense (DOD) domestic crisis manager and was responsible for defense critical infrastructure protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors and was responsible for developing and overseeing the implementation of DOD security policy in the Western Hemisphere. Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation, associate provost of the Naval Postgraduate School, and director of the school's Center for Homeland Defense and Security. Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the author of *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System* (Laurel, MD: JHU/APL, 2016) and numerous other publications. He served as the facilitator of the GridEx IV exercise (November 2017) and is a member of the Homeland Security Advisory Council and other public and private sector boards.









JOHNS HOPKINS  
APPLIED PHYSICS LABORATORY

**From:** [William Harris](#)  
**To:** [directors@resilientsocieties.org](mailto:directors@resilientsocieties.org)  
**Cc:** ["william graham"](#); [Joseph McClelland](#); [David Ortiz](#); ["Melissa Hancock"](#); [Bruce.Walker@hq.doe.gov](mailto:Bruce.Walker@hq.doe.gov); ["Randy Horton"](#)  
**Subject:** Request for greater panelist diversity for FERC Reliability Technical Panels, plus filing of Chairman's Report to EMP Commission in FERC Docket RM18-11-000  
**Date:** Friday, September 07, 2018 4:36:43 PM  
**Attachments:** [Resilient Societies FERC Docket AD18-11-000\\_20180907\\_4pm.pdf](#)

---

## Submission Status

### [Printer Friendly Submission Summary](#)

Submission ID    Bruce

Submission Description    Comment of Foundation for Resilient Societies under AD18-11-000. Requests that selection of future Technical Reliability panelists include more non-industry participants; and submission of Chairman's Report to the EMP Commission, highlighting E3 hazards.

Submission Date    9/7/2018 4:12:24 PM

Filed Date    9/7/2018 4:12:24 PM

Current Status    Pending

Dockets	Docket	Description	Applicant/Filer
	AD18-11-000	NOTICE OF TECHNICAL CONFERENCE	Reliability Technical Conference

Files	Security Level	Filename	Description
	Public	Resilient Societies FERC Docket AD18-11-000_20180907_4pm.pdf	Chairman's Rpt on emp protection & need for diverse panelists

Filing Party/Contacts	Filing Party	Signer (Representative)	Other Contacts (Principal)
	Foundation	williamrharris@yahoo.com	

for Resilient  
Societies

For any issues regarding FERC Online, please contact FERC Online Support or call Local: 202-502-6652 | Toll-free: 866-208-3676. Please include a current mail address, telephone number, and e-mail address.

A handwritten signature in black ink that reads "Wm. R. Harris". The signature is written in a cursive style with a large, stylized "W" and "H".

William R. (Bill) Harris  
Attorney and Director  
Foundation for Resilient Societies  
[williamh@resilientsocieties.org](mailto:williamh@resilientsocieties.org)  
[www.resilientsocieties.org](http://www.resilientsocieties.org)

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

**Reliability Technical Conference**

)

**Docket No. AD18-11-000**

**COMMENTS OF THE FOUNDATION FOR RESILIENT SOCIETIES**

Submitted to FERC on September 7, 2018

The Foundation for Resilient Societies objects to the narrow witness selection for the FERC 2018 Reliability Technical Conference and respectfully requests that the Commission in future years accept the nominations of witnesses who are willing to dissent from electric utility positions and have the technical expertise to do so. Unfortunately, this year's list of witnesses included a few government officials but mostly industry representatives, consultants, and vendors dependent on the electric utility industry for revenues, the only exception being Ms. Alison Silverstein, a consultant who has ridiculed the U.S. Department of Energy's Notice of Proposed Rulemaking for generator fuel security. Ms. Silverstein is a former FERC employee.

When FERC excludes witnesses who challenge industry positions, or those who are not well-connected at FERC, the public interest is not well served. See Appendix 1 for our April 2016 letter to then-FERC Chairman Norman Bay on witness selection for annual electric reliability technical conferences and Appendix 2 for this year's rejected nomination of Mr. Michael Mabee, an example of a potential witness who could have informed the Commission about the societal impact of inadequate electric grid reliability. If a blackout from a High Impact Low Frequency event were to cause societal disruption and large loss of life, the Commission would bear heavy moral responsibility for having given preferred access to industry representatives while excluding others such as Mr. Mabee, an expert and book author on emergency preparedness for blackouts.

It is also unfortunate that no witnesses were present to refute scientifically unfounded testimony regarding the threat to high voltage transformers from the late-time E3 pulse



(electromagnetic pulse, or EMP) generated by high-altitude nuclear detonation. In regard to this threat to transformers, Mr. Robert Bradish of American Electric Power (AEP) testified:<sup>1</sup>

MR. BRADISH: Sure, well I'd certainly like to spend a lot of time talking about ENP [sic: EMP]. Each of our states is very interested in ENP [sic: EMP] also. So from an EPRI perspective and we're very much involved in that work -- in following that work, we're funding some of that work.

You know, they looked at the E-3 already, they did a very detailed, you know, they built on the ENP [sic: EMP]. Commission's work, have improved the modeling and the analysis and you know, their conclusions on the E-3 from -- the initial threat was the ENP [sic: EMP]. would have a significant impact on transformation.

And transformers are long lead time items and so therefore we'd lose all of our transformers, we wouldn't be able to get power, bad things could happen. That analysis, from an E-3 standpoint said they don't see that. They don't see the threat to the transformers. That's not to mean there isn't threats from the ENP [sic: EMP]., there just wasn't that threat to the transformers all failing and us being without power for months on end.

In the *Chairman's Report to the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (Congressional EMP Commission), Dr. Edward B. Savage and Dr. William A. Radasky refuted the findings of the Electric Power Research Institute (EPRI):

The most recent example of industry inadequacy as a champion for EMP preparedness is a study by EPRI that purports to prove a nuclear EMP attack would destroy few, if any EHV transformers. I have reviewed this study and find many flaws in the EPRI assessment. Contrary to EPRI, many EHV transformers would be at risk from the same nuclear EMP attack postulated by EPRI. The EMP Commission has produced a report providing a more realistic assessment of the E3 EMP field strengths likely to be generated by a nuclear EMP attack. The Commission's unclassified assessment of the E3 EMP threat should better inform the electric power industry and other private sector critical infrastructures so they can better protect themselves. *See the EMP Commission Report by Dr. Edward B. Savage and Dr. William A. Radasky, Development of Estimates of Peak Values of the Late-Time (E3) HEMP Heavy Electric Fields Using Measured Data from High Altitude Nuclear Testing* (Metatech: Meta-R-440, July 10, 2017).<sup>2</sup>

---

<sup>1</sup> Federal Energy Regulatory Commission, Transcript of 2018 Reliability Technical Conference Regarding the Bulk-Power System, Docket No. AD18-11-000. July 31, 2018. See p. 113.

<sup>2</sup> Quoted from Dr. William R. Graham, "Chairman's Report to the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," July 2018, at p. 40. The full text of Metatech Report R-440,

The full text of the *Chairman's Report to the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* is included as Appendix 3 of this comment. Pages 39-42 of this document contains a section titled "Regulatory Failures by the U.S. Federal Energy Regulatory Commission, the North American Energy Regulatory Corporation, and the Electric Power Industry." We respectfully ask that the Commissioners and FERC staff read and consider the *Chairman's Report*, now placed in its entirety on FERC Docket No. AD18-11-000.

Respectfully submitted by:



Thomas S. Popik, Chairman

[thomasp@resilientsocieties.org](mailto:thomasp@resilientsocieties.org)



William R. Harris, Secretary,

[williamh@resilientsocieties.org](mailto:williamh@resilientsocieties.org)

**Foundation for Resilient Societies**

52 Technology Way

Nashua, NH 03060-3245

[www.resilientsocieties.org](http://www.resilientsocieties.org)

---

prepared for the year 2017 EMP Commission and referenced in the Chairman's Report of July 2017 is available at the Defense Technical Information Center (DTIC) as "[Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures](#)," July 2017. EPRI's EMP program research team published its assessment of transformer vulnerability to the thermal effects of late-time EMP E3 waveform in February 2017, without considering E1 and E3 interactions and without prior consultation with the year 2017 EMP Commission. In fact, the EMP Commission was not consulted until after publication and a public relations campaign mounted in mid-February 2017. That EPRI Report, by Dr. Randy Horton, et al., entitled "[Magnetohydrodynamic Electromagnetic Pulse Assessment of the Continental U.S. Electric Grid: Magnetically Induced Current and Transformer Thermal Analysis](#)," February 2017 assumed a 24 volt/kilometer peak geoelectric field, compared to the substantially higher 85 volt/kilometer geoelectric field modeled by the year 2017 EMP Commission for locations proximate to the southern border of the CONUS and based upon actual Russian high altitude test experiences over Kazakhstan in year 1962.

**APPENDIX 1—Letter to FERC Chairman Bay**  
**Foundation for Resilient Societies**  
52 Technology Way  
Nashua NH 03060

April 21, 2016

The Honorable Norman C. Bay, Chairman  
Federal Energy Regulatory Commission  
888 First Street, NE  
Washington, DC 20426

**Reference: Dockets No. AD16-15-000, No. RM15-14-000, RM15-11-000**

Dear Chairman Bay:

We are writing to ask that FERC establish an open and balanced process for its Reliability Technical Conference scheduled for June 1 of this year, including inclusion of speakers that may not agree with assertions by the North American Electric Reliability Corporation (NERC) that electric utilities have achieved an “adequate level of reliability.”

Unlike other electric reliability technical conferences, FERC has a practice of not soliciting speaker nominations for this annual event. On April 7<sup>th</sup>, we wrote Ms. Sarah McKinley, contact point for the event, and she forwarded our request for a speaker nomination process to FERC staff. After two full weeks, we have received no reply.

In past years, nearly all speakers have been NERC officials or electric utility executives that promoted the dubious idea that electric reliability is adequate, based on defective statistics developed by NERC. Resilient Societies is willing to engage the services of a professional statistician to independently examine NERC’s statistical methods and present findings at your Reliability Technical Conference. In light of the December cyberattack on the Ukraine electric grid, we would also propose that independent experts on cybersecurity be considered by FERC as potential speakers. Physical security, geomagnetic disturbance, and electromagnetic pulse are other electric reliability issues that could be openly examined by a diversity of speakers.

We hope that FERC grants our request to give opportunity to speakers that may disagree with the positions of NERC and the electric utilities. If not, we will necessarily look to other forums to address our concerns.

Sincerely,



Thomas S. Popik, Chairman  
Foundation for Resilient Societies

cc: FERC Commissioners Tony Clark, Cheryl LaFleur, and Collette Honorable

## **APPENDIX 2—Rejected Nomination of Michael Mabee for 2018 Reliability Technical Conference**

### **Biography:**

Michael Mabee is a national expert on emergency preparedness, specifically on community preparedness for a long-term power outage. He is the author of two books, *The Civil Defense Book: Emergency Preparedness for a Rural or Suburban Community* and *Prepping for a Suburban or Rural Community: Building a Civil Defense Plan for a Long-Term Catastrophe*. Mr. Mabee's career includes experience as an urban emergency medical technician and paramedic, a suburban police officer, and in the federal civil service. In the U.S. Army, Mr. Mabee served in two wartime deployments to Iraq and two humanitarian missions to Guatemala. He retired from the U.S. Army Reserve in 2006 at the rank of Command Sergeant Major (CSM). Mr. Mabee was decorated by both the U.S. Army and the federal government for his actions on 9/11/2001 at the World Trade Center in New York City.

Mr. Mabee has a great deal of experience – both overseas and in the U.S. – working in worlds where things went wrong.

### **Preferred Topics to Address:**

In his proposed testimony, Mr. Mabee would draw on his emergency preparedness knowledge to explain why regulatory steps by FERC to bolster grid resilience are essential. The United States has never experienced a wide-area, long-term outage of the bulk power system and the stakes are dangerously high. Because government and industry tends to prepare for known events (such as hurricanes, earthquakes, tornadoes, local or regional power outages etc.) we are not, as a nation, prepared for wide-area blackouts. In this context, Hurricane Maria and Hurricane Katrina were actually best case scenarios because massive national resources were available to bring into the “disaster area” from unaffected areas.

Mr Mabee proposes to explore plausible scenarios for the 35,000 municipalities and the 326 million people in the U.S. during rolling blackouts or after wide-area cascading collapse. Based on experience during the August 2003 Blackout and Hurricane Sandy, we can expect about one-quarter of emergency generators to fail. A large percent of hospitals, police stations, fire stations, and jails would lose all power. Pharmacies would become targets of opportunity for criminals and drug addicts, especially if load shedding schedules are publicly released in advance. Without traffic signals or officers directing traffic, cars would run out of gas and stall on highways. In winter months, people would take imprudent steps, such as bringing gas grills into their homes for heating. Emergency calls to 911 would explosively increase, especially for with those with diabetes or on dialysis.

Already, ISO New England has posited multiple rolling blackout scenarios by 2025 in their comments for FERC Docket RM18-1-000 on grid resilience. Some scenarios have over 100 hours of load shedding over a week or more. In this context, advance emergency planning by municipalities for rolling blackouts or total grid collapse is essential. For example, municipalities should have special plans for police deployment during blackouts, including guarding of pharmacies and municipal fuel storage. Increased shifts for first responders should be pre-planned, especially when reliability coordinators, balancing authorities, transmission operators, and local distribution companies can give municipalities advance notice of the timing and locations of load shedding.

There are no effective federal or local government plans for wide area, long-term outage and so such an event must be prevented by government and industry action. Proactive steps by FERC can save lives.



**APPENDIX 3 — Dr. William R. Graham, Chairman's Report to the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, July 2017.**

The background of the entire page is a photograph of a sunset or sunrise. The sun is a large, bright, glowing orb in the center of the frame, partially obscured by thin, wispy clouds. The sky is a deep orange-brown color. In the foreground, there is a dark, silhouetted horizon line. On the left side of the horizon, there is a small, dark structure that looks like a lighthouse or a small building with a few lights on top. The overall mood is somber and dramatic.

# Chairman's Report

by

Dr. William R. Graham

**Chairman, Commission to Assess the Threat to the United  
States from Electromagnetic Pulse (EMP) Attack**

July 2017

**Report to the Commission to Assess the Threat to the United States  
November 2017 from Electromagnetic Pulse (EMP) Attack**



REPORT TO THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES  
FROM ELECTROMAGNETIC PULSE (EMP) ATTACK

---

# Chairman's Report

by  
**Dr. William R. Graham, Chairman**  
**Commission to Assess the Threat to the United States from**  
**Electromagnetic Pulse (EMP) Attack**

**July 2017**

The cover photo depicts Fishbowl Starfish Prime at 0 to 15 seconds from Maui Station in July 1962, courtesy of Los Alamos National Laboratory.

This report was produced to support the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. The Commission was established by Congress in the FY2001 National Defense Authorization Act, Title XIV, and was continued per the FY2016 National Defense Authorization Act, Section 1089.

The Commission completed its information-gathering in June 2017. The amended report was cleared for open publication by the Department of Defense Office of Prepublication and Security Review on July 27, 2018.

This report is unclassified and cleared for public release.



## **Acknowledgements**

The author would like to thank Dr. Peter Pry for conducting the research and preparing most of the material in the section on EMP Attack and Combined-Arms Cyber Warfare.

## Acronyms and Abbreviations

AQAP	Al Qaeda in The Arabian Peninsula
BMEWS	Ballistic Missile Early Warning System
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EI	Edison Electric Institute
EHV	extra high voltage
EMP	electromagnetic pulse
EPRI	Electric Power Research Institute
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FERC	Federal Energy Regulatory Commission
FOBS	Fractional Orbital Bombardment System
GAO	Government Accountability Office
GMD	geomagnetic disturbances
HEMP	high-altitude electromagnetic pulse
JAEC	Joint Atomic Energy Intelligence Committee
MNA	Mehr News Agency
NATO	North Atlantic Treaty Organization
NERC	North American Electric Reliability Corporation
PLA	People's Liberation Army
PRC	People's Republic of China
RFW	radio frequency weapon
RMA	revolution in military affairs
SCADA	supervisory control and data acquisition
SHSGA	Homeland Security and Government Affairs Committee

## Table of Contents

Abstract.....	4
Background and Recommendations.....	6
Immediately.....	9
Mid-Term .....	10
Long-Term.....	10
The EMP Commission History .....	12
EMP Attack and Combined-Arms Cyber Warfare .....	17
Russia .....	18
China .....	19
Iran .....	21
North Korea.....	23
Non-Nuclear EMP Weapons.....	26
Physical Attacks on Power Grids.....	27
Cyber-Attacks on Power Grids .....	28
Misinformation about EMP and the North Korean Threat .....	31
North Korea Nuclear EMP Attack: An Existential Threat.....	35
The Fragility of Complex Systems .....	37
Regulatory Failures by the U.S. Federal Energy Regulatory Commission, the North American Energy Regulatory Corporation, and the Electric Power Industry .....	39
The 2014 Intelligence Report.....	43
Conclusions.....	44

## **Abstract**

The United States critical national infrastructure faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, and natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about a high altitude nuclear-weapon generated EMP attack as a tactic by which the Soviet Union could suppress the U.S. national command authority and U.S. strategic forces' ability to respond to a nuclear attack, and thus destroy the U.S. deterrence value of assured nuclear retaliation. Within the last decade, newly-nuclear armed adversaries, including North Korea, have been developing the ability to deploy and threatening to carry out an EMP attack against the U.S. Such an attack would give North Korea and countries that have only a small number of nuclear weapons the ability to cause widespread, long-lasting damage to critical national infrastructures of the United States itself as a viable country and to the survival of a majority of its population.

While during the Cold War major efforts were undertaken by the Department of Defense (DoD) to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack, no major efforts were then thought necessary by the national leadership to protect critical national infrastructures, provided that nuclear deterrence was successful. With the development of small nuclear arsenals and long-range missiles by small, hostile, potentially irrational countries, including North Korea, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the U.S. Therefore, it is critical that the U.S. national leadership address the EMP threat as an immediate, existential issue, and give a high priority to assuring the necessary leadership is engaged and the necessary steps are taken to protect the country from EMP. Otherwise, foreign adversaries may reasonably consider such an attack as one that can gravely damage the U.S. by striking at its technological Achilles' heel, without having to overcome the U.S. military.

Protecting and defending the national electric grid and other critical infrastructures from EMP can be accomplished at reasonable cost and minimal disruption to the present systems that comprise our critical infrastructure; all commensurate with Trump Administration plans to repair and improve U.S. infrastructures, increase their reliability, and strengthen our homeland defense and military capability.

I highly commend President Trump's new executive order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" signed on May 11, 2017. I strongly recommend that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection, since all-out cyber warfare as planned by Russia, China, North Korea, and Iran includes nuclear EMP attack, and integrating EMP and cyber-protection will be both the least expensive and most technically sound approach. Protecting against nuclear EMP will also protect

against natural EMP from solar super storms. The United States should not remain in our current state of existential vulnerability to well-known natural and manmade EMP threats. Such vulnerability invites attack.

The single most important action that must be taken immediately to advance national strength and survivability is:

**Establish an Executive Agent, with the authority, accountability, and resources, to manage U.S. national infrastructure protection and defense against the existential EMP threat.** Current institutional authorities and responsibilities—government, industry, regulatory agencies—are fragmented, incomplete, inexperienced, under-resourced, and unable to protect and defend against foreign hostile EMP threats and solar super-storms.



## Background and Recommendations

### ***WE CAN PREVENT AN EMP CATASTROPHE***

The United States—and modern electric power- and electronic-based civilization more generally—face present and continuing existential threats from naturally occurring and manmade EMP and Combined-Arms Cyber Warfare on our military and on our critical national infrastructures.

**Protecting the national electric grid and other critical infrastructures from the most severe of these threats—nuclear EMP attack—could be done in a manner that protects against other electromagnetic threats, including geomagnetic storms.** Extensively tested, performance-proven technologies for EMP hardening have been developed and implemented by the DoD to protect critical military systems for over 50 years, and can be *affordably* adapted to protect electric grids and other critical infrastructures, at a remarkably low cost relative to that of an EMP catastrophe. Such hardening should be applied in a prioritized manner, with the most important and difficult to replace assets being addressed first. For example, the nuclear reactors providing electric power in the U.S., along with their spent fuel storage facilities, should be given high priority.

**President Trump’s plan to repair and strengthen our national infrastructure, cyber security, homeland defense, and military capability presents an excellent opportunity to include measures for EMP protection that would mitigate the existential threats from solar super-storms and Combined-Arms Cyber Warfare.**

A plausible long term nationwide blackout of the electric power grid and grid-dependent critical infrastructures—e.g., communications, public health, transportation, food-and-water supply—could disable most of our critical supply chains, leaving the U.S. in its condition prior to the advent of electric power in the 19<sup>th</sup> Century, when the national population was less than 60 million, but today without many of the past skills and assets necessary for our population to survive in those conditions. The result could be the death of a large fraction of the American people through the effects of starvation, disease, and societal collapse.

While national planning and preparation for such events could help mitigate the damage, outside the DoD few such actions are currently underway or even being contemplated. The United States, as the most technologically advanced nation in the world, is also the society most dependent upon electricity and electronics for survival and well-being. An extended national-scale blackout and loss of most electricity-dependent infrastructure could be induced by any of several threats:

**Solar super-storms**, like the 1859 Carrington Event, generate natural EMP that could blackout electric grids and other life-sustaining critical infrastructures over remarkably wide areas, putting

at risk the lives of many millions. Recurrence of another Carrington Event is inevitable. The National Aeronautics and Space Administration (NASA) reports the Earth was nearly impacted by a solar super-storm on July 23, 2012. NASA estimates the likelihood of such an event to be 12 percent per decade, virtually guaranteeing Earth will be impacted by a solar super-storm within the lifetimes of our grandchildren—and perhaps ourselves as well.

**Nuclear EMP attack** can be conducted with only a single nuclear weapon detonated at high altitude (a few dozen to several hundred kilometers) delivered either by satellite, a wide variety of long- and short-range missiles including some cruise and anti-ship missiles, a jet doing a zoom-climb, or even a high-altitude balloon. Some modes of such attacks could be executed relatively anonymously, thereby impairing attribution and therefore deterrence. Russia and China now have the capability to conduct a nuclear EMP attack against the U.S., and if not already at hand North Korea will soon have that capability. All have practiced or described contingency plans to do so. Terrorists or other less-sophisticated actors also might mount a nuclear EMP attack if they have access to a suitable nuclear explosive. Missile or other weapon delivery for EMP attack does not require a nuclear weapon re-entry system or accurate missile guidance.

**Sabotage** of the national grid by damaging extra-high-voltage (EHV) transformers using rifles, explosives, or non-nuclear EMP weapons could produce protracted and widespread blackouts by attacking less than a dozen major grid substations, according to the public statements of a past Chairman of the U.S. Federal Energy Regulatory Commission (FERC). At least one substantive rehearsal of such an attack may have already taken place: the sophisticated, damaging attack of the Metcalf electric substation in the San Francisco Bay Area.

**Combined-Arms Cyber Warfare**, as planned by Russia, China, North Korea, and Iran may use combinations of cyber-, sabotage-, and ultimately nuclear EMP-attack to impair the United States quickly and decisively by blacking-out large portions of its electric grid and other critical infrastructures. Foreign adversaries may also consider nuclear EMP attack as the ultimate cyber “denial of service” weapon, one which can gravely damage the U.S. by striking at its technological Achilles’ heel, without having to engage the U.S. military. The synergism of such combined-arms is described in the military doctrines of all these potential adversaries as the greatest Revolution in Military Affairs (RMA) in history—one which anticipates rendering obsolete many, if not all, traditional instruments of military power.

**While I highly commend President Trump’s new Executive Order “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” signed on May 11, 2017, I strongly recommend that implementation of cybersecurity for the electric grid and other critical infrastructures include EMP protection, since all-out cyber warfare as planned by Russia, China, North Korea, and Iran includes nuclear EMP attack.** However, current institutional arrangements for protecting and improving the reliability of the electric grids and other critical infrastructures through the U.S. FERC and the North American Electric Reliability

Corporation (NERC) are not designed to address major national security threats to the electric power grids and other national critical infrastructures. Using the U.S. FERC and NERC to achieve this level of national security is beyond the purpose for which those organizations were created and has proven to be fundamentally unworkable; new institutional arrangements are needed to advance preparedness to survive EMP and related threats to our critical national infrastructures.

I continue to recommend that U.S. critical national infrastructures be protected from EMP as outlined in our unclassified reports provided in 2004 and 2008, and elsewhere. Additional recommendations are provided in the present report. The single most important action that must be taken urgently to advance national strength and survivability is:

**Establish an Executive Agent—a Cabinet Secretary designated by the President—with the authority, accountability, and resources, to manage U.S. national infrastructure protection and defense against EMP and the other existential threats described above.** Current institutional authorities and responsibilities—government, industry, regulatory agencies—are fragmented, incomplete, and unable to protect and defend against foreign hostile EMP threats and solar super-storms.

Additionally:

**I encourage the President to work with Congressional leaders to stand-up a Joint Presidential-Congressional Commission, with its members charged with supporting the Nation's leadership and providing expertise, experience, and oversight to achieve, on an accelerated basis, the protection of critical national infrastructures.** The U.S. FERC and NERC have for nearly a decade been unable or unwilling to implement the EMP Commission's recommendations. A Presidential-Congressional Commission on Critical Infrastructure Protection could engage the Free World's preeminent experts on EMP and Combined-Arms Cyber Warfare to serve the entire Government in a manner akin to the Atomic Energy Commission of the 1947-74 period, advising the Administration regarding actions to attain most quickly and most cost-effectively the protection essential to long-term national survival and wellbeing. The United States should not remain in our current state of fatal vulnerability to well-known natural and man-made threats.

I recommend, given the proximity and enormity of the threat from EMP and Combined-Arms Cyber Warfare, the President exercise leadership to implement immediate, mid-term, and long-term steps to deter and defeat this existential threat.

### *Immediately*

*I recommend that the President declare that EMP or cyber-attacks that blackout or threaten to blackout the national electric grid constitute the use of weapons of mass destruction that justify preemptive and retaliatory responses by the United States using all possible means, including nuclear weapons.* Some potential adversaries have the capability to produce a protracted nationwide blackout induced by EMP and other elements of Combined-Arms Cyber Warfare. A Defense Science Board study *Resilient Military Systems and the Advanced Cyber Threat* (January 2013) equates an all-out cyber-attack on the United States with the consequences of a nuclear attack, and concludes that a nuclear response is justified to deter or retaliate for cyber warfare that threatens the life of the nation: “While the manifestations of a nuclear and cyber-attack are very different, in the end, the existential impact to the United States is the same.”

*I recommend that the President issue an Executive Order titled “Protecting the United States from Electromagnetic Pulse (EMP) Attack.”* Among many other provisions to protect the nation from EMP on an emergency basis, the Executive Order would instantly mobilize a much needed “whole of government solution” to the EMP and combined-arms cyber threat: “All U.S. Government Departments, Agencies, Offices, Councils, Boards, Commissions and other U.S. Government entities...shall take full and complete account of the EMP threat in forming policies and plans to protect United States critical infrastructures...” Protecting the electric grid and other critical infrastructures from the worst threat—nuclear EMP attack—can, if carried out in a system-wide, integrated approach, help mitigate all lesser threats, including natural EMP, man-made non-nuclear EMP, and cyber-attack, physical sabotage, and severe solar and terrestrial weather.

*I recommend that the President direct the Secretary of Defense to include a Limited Nuclear Option for EMP attack among the U.S. nuclear strike plans, and immediately assure targeting and fusing capabilities for some of the nuclear forces to implement a nuclear EMP attack capability.*

[REDACTED]

[REDACTED]

[REDACTED] If either or both of these satellites are nuclear-armed, they should be intercepted and destroyed over a broad ocean area where an EMP resulting from possible salvage-fusing will do the least damage.

*I recommend that the President direct the Secretary of Defense to post Aegis ships in the Gulf of Mexico and near the east and west coasts, and the Secretary in turn should direct them to be prepared to intercept missiles from freighters, submarines, or other platforms that might launch a nuclear EMP attack on the United States.* Ground-based U.S. National Missile Defenses (NMD) are primarily located in Alaska and California and oriented for a missile attack coming at

the U.S. from the north, and are not deployed to intercept a missile attack launched near the U.S. coasts or from the south.

*I recommend that the President direct the Secretary of Homeland Security to harden the FirstNet emergency communications system against EMP.*

*I recommend that the President initiate Training, evaluating, and “Red Teaming” efforts to prepare the U.S., and in the event of an EMP attack to respond, and periodically report the results of these efforts and the state or national readiness to the Congress.*

### ***Mid-Term***

I recommend that the President direct the Secretary of Defense to deploy Aegis-ashore missile interceptors along the Gulf of Mexico coast to fill the gap in U.S. missile defenses. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

I recommend that the President direct the Secretary of Defense to develop a space-surveillance program to determine if any satellites orbited over the United States are nuclear-armed, and develop space-interception capabilities to defend against nuclear-armed satellites that might make an EMP or other attack.

*I recommend that the President direct the Nuclear Regulatory Commission to launch a crash program to harden the active nuclear power reactors and all spent fuel storage facilities against nuclear EMP attack.* Even if the reactors and storage facilities survive an initial EMP attack, they currently are not able to restart generating power if there is no electric power available on its grid, and they typically only have enough emergency power to cool reactors and spent fuel facilities for several days, after which they would “go Fukushima,” spreading radioactivity over adjacent areas.

### ***Long-Term***

*The Commission recommends that the President through his Executive Agent protect elements of the national electric grid, the keystone critical infrastructure upon which all other critical infrastructures depend.* Priority should be given to elements that are difficult and time-consuming to replace. Such elements can be protected from EMP at very low cost relative to the cost of an EMP catastrophe, and paid for without federal dollars by a slight increase in electric rates.

*I recommend that a similar approach be taken to key elements of the national telecommunications infrastructure and other national critical infrastructures.*



### ***Progress Made by the Department of Defense***

The statute re-establishing the EMP Commission directs it to evaluate and report on:

- (1) The vulnerability of electric-dependent military systems in the United States to a manmade or natural EMP event, giving special attention to the progress made by the Department of Defense, other Government departments and agencies of the United States, and entities of the private sector in taking steps to protect such systems from such an event.***

The DoD has been the primary federally funded organization to analyze, develop models, simulate, develop hardening technology, and using resources provided to it, to strengthen U.S. national security. The DoD has in the past sponsored much excellent work in these areas; however, even though it is the most knowledgeable federal agency in the field of EMP, it has:

1. Failed to transfer much of its technical capabilities and accomplishments to other agencies of the federal government;
2. Failed to use its knowledge to assist and critique activities of other federal agencies, including the intelligence community;
3. Failed to declassify EMP environment and effects data and predictions that, while known to U.S. adversaries, are not available to the U.S. public, U.S. infrastructure organizations, and U.S. professional societies that develop specifications and standards for protecting critical national infrastructure;
4. Failed to obtain the complete archive of Russian nuclear weapons effects data when offered for sale to the U.S. at modest cost in 1996;
5. Failed to inform the Congress and the public of the present and continuing existential EMP threat to the nation; and
6. Failed to develop and pursue plans to protect the U.S. from EMP threats.

Overall, for more than a decade, the DoD has been derelict in its duties to lead the country in providing for national defense and security from EMP attack. This dereliction of duty should not be allowed by the leadership of the Administration and the Congress to continue.

*I recommend the development and deployment of enhanced-EMP nuclear weapons and other means to deter adversary attack on the United States. Enhanced-EMP nuclear weapons, called by the Russians Super-EMP weapons, can be developed without nuclear testing.*

*I recommend strengthening U.S. ballistic missile defense, deploying it to protect the U.S. from attack from near-by oceans as well as from longer distances, including by development and deployment of space-based defenses.*

## The EMP Commission History

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack was first established by Congress in the FY2001 Floyd D. Spence National Defense Authorization Act, Title XIV, following 5 years of classified and unclassified hearings by Congress to ascertain if Russia, China, rogue states or terrorists had plans and capabilities to make an EMP attack. The final impetus to establish the EMP Commission was provided in April 1999, during the bombing of former Yugoslavia by the North Atlantic Treaty Organization (NATO), when a congressional delegation meeting in Vienna to discuss the Balkans crisis with senior members of the Russian Duma were threatened with a “hypothetical” nuclear EMP attack against the United States.

Under the Congressional EMP Commission’s original statutory charter, Public Law 106-398, Title XIV, Section 1402 Duties of Commission:

***(a) Review of EMP Threat. The Commission shall assess:***

- (1) the nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years;*
  - (2) the vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness;*
  - (3) the capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack; and*
  - (4) the feasibility and cost of hardening select military and civilian systems against EMP attack.*
- (b) Recommendation. The Commission shall recommend any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack.*

Between 2001 and 2008, the Congressional EMP Commission produced several reports addressing the EMP threat to U.S. military systems and making recommendations. The EMP Commission produced two unclassified reports addressing EMP threats to critical national infrastructures:

*Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume I: Executive Report (2004)*

*Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures (2008)*

The above unclassified reports on civilian critical infrastructures addressed EMP threats to:

- infrastructure commonalities, including Supervisory Control And Data Acquisition (SCADA) systems,
- electric power, identified as the “keystone critical infrastructure” upon which all others depend,
- telecommunications,
- banking and finance,
- petroleum and natural gas,
- transportation,
- food,
- water,
- emergency services,
- space systems, and
- government.

The EMP Commission *Executive Report* summarized the problem as below:

*Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated EMP. A determined adversary can achieve an EMP attack capability without having a high level of sophistication.*

*EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of U.S. society, as well as to the ability of the United States and Western nations to project influence and military power.*

*The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled through critical infrastructures. Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The impact of EMP is asymmetric in relation to potential protagonists who are not as dependent on modern electronics.*

*The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish.*

The Congressional EMP Commission 2004 *Executive Summary* stated in “Overview: EMP Is Capable of Causing Catastrophe for The Nation” several additional salient points about the nuclear EMP threat:

- *The recovery of any one of the key national infrastructures is dependent on the recovery of others. The longer the outage, the more problematic and uncertain the recovery will be. It is possible for the functional outages to become mutually reinforcing until at some point the degradation of infrastructure could have irreversible effects on the country's ability to support its population.*
- *EMP effects from nuclear bursts are not new threats to our nation...What is different now is that some potential sources of EMP threats are difficult to deter—they can be terrorist groups that have no state identity, have only one or a few weapons, and are motivated to attack the U.S. without regard for their own safety.*
- *Rogue states, such as North Korea and Iran, may also be developing the capability to pose an EMP threat to the United States, and may also be unpredictable and difficult to deter.*
- *Certain types of relatively low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter-century.*
- *China and Russia have considered limited nuclear attack options that, unlike their Cold War plans, employ EMP as the primary or sole means of attack.*
- *Another key difference from the past is that the U.S. has developed more than most other nations as a modern society heavily dependent on electronics, telecommunications, energy, information networks, and a rich set of financial and transportation systems that leverage modern technology.*
- *Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack.*

The Congressional EMP Commission 2008 report *Critical National Infrastructures* made over 100 recommendations to protect the civilian critical infrastructures from nuclear EMP attack and other hazards. The EMP Commission endorsed an “all hazards” strategy as the most cost-effective approach to protecting the critical infrastructures, wherever possible using measures that would safeguard against multiple threats—including nuclear EMP, natural EMP or geomagnetic disturbance (GMD) from solar storms, intentional and accidental electromagnetic interference, cyber-attack, sabotage, and severe weather.

While the Congressional EMP Commission accurately described nuclear EMP attack as an existential threat to the United States, the thrust of the Commission's 2004 and 2008 reports was to recommend how to protect the nation cost-effectively, noting that protection is possible "and well within the Nation's means and resources to accomplish."

Congressional efforts to re-authorize the EMP Commission became more urgent because of misleading and inaccurate reports that are impeding implementation of the EMP Commission recommendations and are making the nation more vulnerable. For example:

- The NERC and the Edison Electric Institute (EEI) in 2012 and subsequently published a series of reports underestimating EMP threats from nuclear attack and from solar storms. These resulted in approval by the U.S. FERC of an inadequate natural EMP and GMD Standard for protecting electric grids, and impeded initiatives by several States to protect their grids from EMP.
- The Joint Atomic Energy Intelligence Committee in 2014 published a report on the EMP threat that is factually inaccurate and deeply flawed analytically, and has impeded implementation of EMP Commission recommendations.
- In 2016, the Electric Power Research Institute (EPRI), which is funded by the electric power industry, published an erroneous report that significantly underestimates the nuclear E3 EMP threat to electric grids. EPRI and others have used the report to lobby against Federal and State initiatives to protect the electric grid against nuclear EMP attack.
- In 2016, a report by the U.S. Government Accountability Office (GAO) concluded, "[U.S. Department of Homeland Security] DHS and [U.S. Department of Energy] DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks." Congressional hearings subsequently confirmed that little or nothing has been done to implement EMP Commission recommendations to protect the electric grid.

Moreover, since the EMP Commission terminated in 2008, growing geopolitical instability, increased risk of war in the Middle East, Asia, and Europe, increasing threats from global terrorism, and increased awareness of natural EMP threats from the Sun—all have heightened congressional concerns about dangers to the electric grid from EMP and other threats. For example:

- North Korea in 2012 and 2016, amidst threats to annihilate the United States and a rapidly advancing nuclear missile program, orbited two satellites in polar orbits that cross over the U.S. on trajectories consistent with practice or preparation for a surprise nuclear EMP attack.
- On June 9, 2014, Al Qaeda in the Arabian Peninsula sabotaged the Yemen electric grid, inducing a temporary nationwide blackout of 19 cities and 24 million people. It is the first time in history that a terror attack has blacked-out an entire nation.



- On March 31, 2015, Turkey experienced a temporary nationwide blackout, allegedly from a cyber-attack by Iran, later denied by the Turkish government. On December 23, 2015, Western Ukraine was blacked-out temporarily by a cyber-attack from Russia. One of these is the first time in history that a large-scale blackout has been induced by cyber-attack.
- On July 23, 2012, the Earth was narrowly missed by a large coronal mass ejection from the Sun that NASA assessed could have caused a protracted worldwide blackout with potentially catastrophic consequences. NASA estimates the likelihood of a potentially catastrophic worldwide natural EMP event from a solar super-storm is 12 percent per decade.

In response to these events and others, Congress re-established the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack in the FY2016 National Defense Authorization Act, Section 1089. The renewed EMP Commission has a broader agenda, to assess threats to the U.S. military and civilian critical infrastructures from nuclear EMP, non-nuclear EMP weapons, cyber-attack, sabotage, and solar storms:

*(d) Expanded PURPOSE. —Section 1401(b) of the Commission charter (114 Stat. 1654A–345) is amended by inserting before the period at the end the following: “, from non-nuclear EMP weapons, from natural EMP generated by geomagnetic storms, and from proposed uses in the military doctrines of potential adversaries of using EMP weapons in combination with other attack vectors.”*

*(e) DUTIES OF COMMISSION. —Section 1402 of the Commission charter (114 Stat. 1654A–346) is amended to read as follows:*

**SEC. 1402. DUTIES OF COMMISSION.**

*The Commission shall assess the following:*

- (1) The vulnerability of electric-dependent military systems in the United States to a manmade or natural EMP event, giving special attention to the progress made by the Department of Defense, other Government departments and agencies of the United States, and entities of the private sector in taking steps to protect such systems from such an event.*
- (2) The evolving current and future threat from state and non-state actors of a manmade EMP attack employing nuclear or non-nuclear weapons.*
- (3) New technologies, operational procedures, and contingency planning that can protect electronics and military systems from the effects of a manmade or natural EMP event.*
- (4) Among the States, if State grids are protected against manmade or natural EMP, which States should receive highest priority for protecting critical defense assets.*
- (5) The degree to which vulnerabilities of critical infrastructure systems create cascading vulnerabilities for military systems.*

## EMP Attack and Combined-Arms Cyber Warfare

Nuclear EMP attack is part of the military doctrines, plans and exercises of Russia, China, North Korea, and Iran for a revolutionary new way of warfare against military forces and civilian critical infrastructures by cyber, sabotage, and EMP. This new way of warfare is called many things by many nations. In Russia, China, and Iran it is called Sixth Generation Warfare, Non-Contact Warfare, Electronic Warfare, Total Information Warfare, and Cyber Warfare. Some U.S. analysts—the very small number paying attention—call it Cybergeddon, Blackout War, or Combined-Arms Cyber Warfare.<sup>1</sup>

Significantly, EMP attack entails detonating a nuclear weapon at such high altitude that no blast or other prompt effects injurious to humans are delivered other than possible eye burn to those looking near the burst point. Since EMP immediately damages only electrical and electronics components and systems, potential adversaries do not appear to regard nuclear EMP attack as an act of nuclear warfare.

Potential adversaries understand that millions could die from the long-term collateral effects of EMP and cyber-attacks that cause protracted black-out of national electric grids and other life-sustaining critical infrastructures. At least some regard this relatively easy, potentially anonymous, method of inflicting mass destruction as an attractive feature of what they describe as a Revolution in Military Affairs.

Ignorance of the military doctrines of potential adversaries and a failure of U.S. strategic imagination, as noted in military writings of potentially hostile powers, is setting America up for an EMP Pearl Harbor.<sup>2</sup> Russia, China, North Korea and Iran appear to regard nuclear EMP attack as the ultimate weapon in an all-out cyber operation aimed at defeating U.S. and allied military forces on the battlefield and in a theater of operations. They also see EMP and Combined-Arms Cyber Warfare as a means of defeating entire nations by blacking-out their electric grids and other critical infrastructures for longer periods of time than technologically developed societies, including the U.S., can tolerate without major disruption and loss of life.<sup>3</sup>

---

<sup>1</sup> While many analysts are paying attention to cyber warfare, narrowly defined as the use of computer viruses and hacking and other such techniques, relatively few conceive of “cyber warfare” as potential adversaries do— as Combined-Arms Cyber Warfare entailing coordinated use of computer viruses etc., sabotage and kinetic attack, non-nuclear and nuclear EMP weapons. Dr. Peter Vincent Pry, *Blackout Wars* (Task Force on National and Homeland Security, 2015), Chapter II “The Blackout War”.

<sup>2</sup> For Example: Zhang Shouqi and Sun Xuegui, “Be Vigilant Against ‘Pearl Harbor’ Incident in The Information Age” Jiefangjun Bao (Official newspaper of the PRC People’s Liberation Army, May 14, 1996).

<sup>3</sup> Ambassador R. James Woolsey, “Heading Toward An EMP Catastrophe” Statement for the Record before the Senate Homeland Security and Governmental Affairs Committee, July 22, 2015.

## *Russia*

For example, Russian General Vladimir Slipchenko in his military textbook *Non-Contact Wars* describes the combined use of cyber viruses and hacking, physical attacks, non-nuclear EMP weapons, and ultimately nuclear EMP attack against electric grids and critical infrastructures as a new way of warfare that is the greatest Revolution in Military Affairs in history. Like Nazi Germany's Blitzkrieg (“Lightning War”) Strategy that coordinated airpower, armor, and mobile infantry to achieve strategic and technological surprise that nearly defeated the Allies in World War II, the New Blitzkrieg is, literally and figuratively, an electronic “Lightning War” so potentially decisive in its effects that an entire civilization could be overthrown in hours.<sup>4</sup>

According to General Slipchenko, EMP and the new RMA renders obsolete modern armies, navies and air forces. For the first time in history, small nations or even non-state actors can humble the most advanced nations on Earth.

An article in *Military Thought*, the flagship journal of the Russian General Staff, “Weak Points of the U.S. Concept of Network-Centric Warfare” points to nuclear EMP attack as a means of defeating the United States: “American forces may be vulnerable to electronic warfare attacks, in particular, an electromagnetic pulse that is a brief powerful electromagnetic field capable of overloading or destroying numerous electronic systems and high-tech microcircuits that are very sensitive to the electromagnetic field, even if transmitted from a distance. A single low-yield nuclear weapon exploded for this purpose high above the area of combat operations can generate an electromagnetic pulse covering a large area and destroying electronic equipment without loss of life that is caused by the blast or radiation.”<sup>5</sup>

Moreover: “Today, too, a considerable body of administrative information in the U.S. armed forces goes through the civilian Internet. Many commercial communication satellites, particularly satellites in low orbits, can have their functions impaired or they can be disabled by electromagnetic shocks from high altitudes.”<sup>6</sup>

A 2015 article from Russia’s A.A. Maksimov Scientific Research Institute for Space Systems, alludes to low-yield nuclear enhanced-EMP as the most effective cyber weapon: “Even more effective are remote-controlled cyber weapons in the nuclear variant, but in this case a warhead

---

<sup>4</sup> Major General Vladimir Ivanovich Slipchenko, *Non-Contact Wars* (Moscow: 2000). See also Slipchenko, *Future War* (Moscow Public Science Foundation, 1999).

<sup>5</sup> Colonel A.V. Kopylov, “Weak Points of the U.S. Concept of Network-Centric Warfare” *Military Thought* (Moscow: Volume 3, 2011).

<sup>6</sup> Ibid.

is required with a capacity many times smaller by comparison with the charges of the typical strategic missiles.”<sup>7</sup>

Russia’s then First Deputy Minister of Defense, Andrey Kokoshin, in a 1997 interview, claimed Russia was developing nuclear weapons “that have no counterparts in the world,” including something that sounds suspiciously like a Super-EMP weapon: “ultra-small nuclear warheads weighing less than 90 kilograms, which are already being manufactured...and radiofrequency weapons.”<sup>8</sup> In Russian military writings, the phrase “radiofrequency weapons” is used to describe nuclear or non-nuclear weapons designed to destroy enemy electronics by means of EMP.

### *China*

China's military doctrine sounds an identical theme. According to People's Liberation Army Textbook *World War, the Third World War—Total Information Warfare*, written by Shen Weiguang (allegedly, according to the People’s Republic of China (PRC), the inventor of Information Warfare), “Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies...”:

*With their massive destructiveness, long-range nuclear weapons have combined with highly sophisticated information technology and information warfare under nuclear deterrence....Information war and traditional war have one thing in common, namely that the country which possesses the critical weapons such as atomic bombs will have “first strike” and “second strike retaliation” capabilities....As soon as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will ground to a halt. Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies in order to equip China without delay with equivalent deterrence that will enable it to stand up to the military powers in the information age and neutralize and check the deterrence of Western powers, including the United States.*

An article “Overview of Electromagnetic Pulse Weapons and Protection Techniques Against Them” from the People’s Republic of China Air Force Engineering University describes nuclear EMP weapons as the most powerful and effective variant of electronic warfare weapons for waging Information Warfare. Nuclear and non-nuclear EMP weapons in the context of

---

<sup>7</sup> Dr. Grigoriy Vokin, Department Chief, “Remote Custodian. Warheads with Artificial Intelligence for Reconnaissance, Guaranteed Destruction of Targets, and Human Rescue” A.A. Maksimov Scientific Research Institute for Space Systems (2015).

<sup>8</sup> Denis Baranets, *Komsomolskaya Pravda* (7 August 1997), p. 1.

Information Warfare are the crucial instruments for implementing this Revolution in Military Affairs:

*In future high-tech warfare under informatized conditions, information warfare will span multiple dimensions, including ground, sea, air, and the EM spectrum. Information superiority has already become central and crucial to achieving victory in warfare...If the communications equipment used for the transmission of battlefield information were attacked and damaged by an opponent's EMP weapons, then the one attacked would face the danger of disruption in battlefield information transmission. EMP severely restricts the tactical performance and battlefield survivability of informatized equipment.<sup>9</sup>*

Moreover, the article clearly makes a distinction between nuclear weapons and nuclear EMP weapons, describing the latter as “a new type of weapon” like non-nuclear EMP weapons for waging Information Warfare:

*As opposed to conventional and nuclear weapons, EMP weapons are a new type of weapon capable of causing mass destruction by instantly releasing high-intensity EMP...They can interfere, damage, and overheat electronics, resulting in logic circuit dysfunctions, control malfunctions, or total failure. The unique destructive effect that EMP have on electronic equipment was unintentionally discovered by the United States in the 1960s during a nuclear test. In July 1962, the United States conducted a high-altitude nuclear explosion in the Pacific Ocean. This...unexpectedly overloaded the Honolulu power grid in Hawaii, 1,400 km away, even overheating lightning protection devices on powerlines. On a battlefield, this new-type weapon will cause devastating damage to electronic systems, including computers, communications and control systems, and radars, resulting in immeasurable losses.<sup>10</sup>*

Furthermore, according to the article: “There are 3 types of military EMP based on pulse sources: the first is the high-altitude electromagnetic pulse (HEMP) produced by the detonation of a low yield nuclear bomb in the atmosphere at high-altitude; the second is...produced by high explosives and related devices; the third is the HPM...produced by HPM devices such as magnetrons and vircators.” Nuclear EMP weapons are, or include, Enhanced-EMP or so-called Super-EMP weapons designed to produce gamma rays and high-frequency E1 EMP: “HEMP weapons are a type of weak nuclear explosive EMP bomb that produces EMP through the detonation of low-yield nuclear bombs at high-altitudes (70 to 100 km above ground).” The E1

---

<sup>9</sup> Zhao Meng, Da Xinyu, and Zhang Yapu, “Overview of Electromagnetic Pulse Weapons and Protection Techniques Against Them” Winged Missiles (PRC Air Force Engineering University: May 1, 2014).

<sup>10</sup> Ibid.



EMP field “produced by nuclear EMP is about 10 to 100 kV/m and can penetrate and melt any electronic components.”<sup>11</sup>

A January 2016 article “General Trend of the Worldwide Revolution in Military Affairs and the Form of Future War” by China’s National Security Policy Committee sees “electromagnetic pulse bombs” among the new “disruptive technologies” that “can change the ‘rules of the game’” by disrupting U.S. military “precision warfare capabilities centered on information technology” thereby sounding “the horn of a new round of revolution in military affairs.”<sup>12</sup>

### *Iran*

A recently translated military textbook ironically titled *Passive Defense* by the Army of the Islamic Republic of Iran (Martyr Lt. General Sayed Shirazi Center for Education and Research, 2010) endorses the theories of Russian General Slipchenko (who is acknowledged on page one of the first chapter).<sup>13</sup> The military manual notes the potentially decisive effects of nuclear EMP attack to defeat an adversary in more than 20 passages. Ambassador R. James Woolsey, former Director of Central Intelligence, writes:

*“Death to America” is more than merely an Iranian chant—Tehran’s military is planning to be able to make a nuclear EMP attack....Rep. Trent Franks quoted from an Iranian military textbook recently translated by the Defense Intelligence Agency’s National Intelligence University...The official Iranian military textbook advocates a revolutionary new way of warfare that combines coordinated attacks by nuclear and non-nuclear EMP weapons, physical and cyber-attacks against electric grids to blackout and collapse entire nations. Iranian military doctrine makes no distinction between nuclear EMP weapons, non-nuclear radio-frequency weapons and cyber-operations—it regards nuclear EMP attack as the ultimate cyber weapon.*<sup>14</sup>

EMP is most effective at blacking-out critical infrastructures, while it does not directly damage the environment or harm human life, according to Iran’s *Passive Defense*:

*As a result of not having the other destructive effects that nuclear weapons possess, among them the loss of human life, weapons derived from electromagnetic pulses have attracted attention with regard to their use in future wars...The superficiality of secondary damage sustained as well as the*

---

<sup>11</sup> Ibid.

<sup>12</sup> Li Bingyan, “General Trend of the Worldwide Revolution in Military Affairs and the Form of Future War” Guangming Ribao Online (January 27, 2016).

<sup>13</sup> Army of the Islamic Republic of Iran, *Passive Defense: Approach to the Threat Center* (Tehran: Martyr Lt. General Sayad Shirazi Center for Education and Research, Spring 2010).

<sup>14</sup> “A Shariah-Approved Nuclear Attack” Washington Times, September 15, 2015.

*avoidance of human casualties serves as a motivation to transform this technology into an advanced and useful weapon in modern warfare.*<sup>15</sup>

Former CIA Director Woolsey notes: “Because EMP destroys electronics directly, but people indirectly, it is regarded by some as Shariah-compliant use of a nuclear weapon. *Passive Defense* and other Iranian military writings are well aware that nuclear EMP attack is the most efficient way of killing people, through secondary effects, over the long run. The rationale appears to be that people starve to death, not because of EMP, but because they live in materialistic societies dependent upon modern technology.”<sup>16</sup>

An Iranian political-military journal, in an article entitled “Electronics To Determine Fate Of Future Wars,” states that the key to defeating the United States is EMP attack and that, “If the world’s industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years...”:

*Advanced information technology equipment exists which has a very high degree of efficiency in warfare. Among these we can refer to communication and information gathering satellites, pilotless planes, and the digital system.... Once you confuse the enemy communication network you can also disrupt the work of the enemy command and decision-making center. Even worse, today when you disable a country’s military high command through disruption of communications you will, in effect, disrupt all the affairs of that country.... If the world’s industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years.... American soldiers would not be able to find food to eat nor would they be able to fire a single shot.*<sup>17</sup>

Ironically, while electric power lobbyists are resisting EMP protection of the U.S. grid in Washington, the Iranian Mehr News Agency reported that Iran is violating international sanctions and going full bore to protect itself from a nuclear EMP attack:

*Iranian researchers...have built an Electromagnetic Pulse (EMP) filter that protects country’s vital organizations against cyber attack. Director of Kosar Information and Communication Technology Institute Saeid Rahimi told [Mehr News Agency] MNA correspondent that the EMP (Electromagnetic Pulse) filter is one of the country’s boycotted products and until now procuring it required considerable costs and various strategies. “But recently Kosar ICT...has managed to domestically manufacture the EMP filter for the very first time in*

---

<sup>15</sup> Ibid.

<sup>16</sup> Ibid

<sup>17</sup> Tehran, Nashriyeh-e Siasi Nezami, December 1998 -January 1999.

*this country,” said Rahimi. Noting that the domestic EMP filter has been approved by security authorities, Rahimi added “the EMP filter protects sensitive devices and organizations against electromagnetic pulse and electromagnetic terrorism.” He also said the domestic EMP filter has been implemented in a number of vital centers in Iran.<sup>18</sup>*

### **North Korea**

North Korea appears to have practiced the military doctrines described above against the United States—including possibly by simulating a nuclear EMP attack and Combined-Arms Cyber Warfare operation against the U.S. mainland.<sup>19</sup>

Following North Korea’s third illegal nuclear test in February 2013, North Korean dictator Kim Jong-Un repeatedly threatened to make nuclear missile strikes against the U.S. and its allies. In what was then the worst ever nuclear crisis with North Korea, that lasted months, the U.S. responded by beefing-up National Missile Defenses and flying B-2 bombers in exercises just outside the Demilitarized Zone to deter North Korea.<sup>20</sup>

On April 16, 2013, North Korea’s KMS-3 satellite orbited over the U.S. from a south polar trajectory, over-flying the Washington, DC-New York City corridor, the nation’s political and economic capitals, from the south. [REDACTED]

[REDACTED] On April 16, KMS-3’s trajectory was near optimal to make an EMP attack that could blackout the Eastern Grid that services half of the United States—if the satellite is nuclear-armed. On that same day, parties unknown used AK-47s to make a sophisticated commando-style attack on the Metcalf transformer substation, which services San Francisco and the Silicon Valley, an important part of the Western grid. Cyber-attacks on U.S. critical infrastructures continued throughout the crisis.<sup>21</sup>

On January 6, 2016, North Korea provoked another nuclear crisis with its fourth illegal nuclear test of what it claimed was an H-Bomb. On February 7th, again amidst threats to make a nuclear

---

<sup>18</sup> "Iran Builds EMP Filter For 1st Time" Mehr News Agency, June 13, 2015.

<sup>19</sup> "EMP Threat from North Korea, 2013" Family Security Matters, April 27, 2014.

<sup>20</sup> "U.S. Warns North Korea With Stealth Bomber Flights" Wall Street Journal, March 29, 2013.

<sup>21</sup> "EMP Threat from North Korea, 2013" op. cit.; KMS-3 is NORAD's acronym for North Korea's satellite Kwangmyongsong-3 (Lodestar-3 or Guiding Star-3), a name richly symbolic for Korean mythology and the deification of Kim Jong-Un who according to official propaganda was born on Mt. Paeku under a newly appeared bright guiding star, signifying the birth of a great general. KMS-3 was launched on December 12, 2013, exactly two months before, and probably in anticipation of, North Korea’s illegal nuclear test on February 12, 2013.

### *Are North Korea's Satellites an EMP Threat?*

North Korea's KMS-3 and KMS-4 satellites orbit over the U.S. daily. [REDACTED]

[REDACTED] Their trajectory is similar to that planned for a Soviet-era secret weapon called the Fractional Orbital Bombardment System (FOBS) deployed by the USSR to make a surprise nuclear attack on the United States. In 2004, two retired Russian generals, then teaching at Russia's Voroshilov General Staff Academy, told the EMP Commission that the design for Russia's Super-EMP nuclear weapon was accidentally transferred by Russian scientists and engineers working on North Korea's missile and nuclear weapons program. They said North Korea could test a Super-EMP weapon "in a few years." The 2006 and subsequent low-yield tests do not appear to have been failures because North Korea proceeded with weaponization. In 1997, Andrey Kokoshin, then Russia's First Deputy Defense Minister, stated Russia was deploying a new generation of advanced nuclear weapons "that have no counterparts in the world" including EMP weapons and "ultra-small warheads weighing less than 90 kilograms." Such weapons would be small enough for North Korea's satellites. General Vladimir Slipchenko and General Vladimir Belous, who warned the EMP Commission about North Korean development of Super-EMP weapons, are among Russia's most prominent military scientists and experts on EMP and advanced technology warfare. General Slipchenko's advocacy of EMP and Combined-Arms Cyber Warfare is recognized in Iran's military textbook *Passive Defense* that advocates development of capabilities for nuclear EMP attack.

missile strike on the United States, Pyongyang orbited another satellite, the KMS-4, on the same polar trajectory as the KMS-3.<sup>22</sup>

Kim Jong-Un has threatened to reduce the United States to "ashes" with "nuclear thunderbolts" and threatened to retaliate for U.S. diplomatic and military pressure by "ordering officials and scientists to complete preparations for a satellite launch as soon as possible" amid "the enemies' harsh sanctions and moves to stifle" the North.<sup>23</sup> North Korean press asserts readiness for "any form of war" and includes their satellite with "strengthening of the nuclear deterrent and legitimate artificial satellite launch, which are our fair and square self-defensive choice."

Moreover: "The nuclear [weapons] we possess are, precisely, the country's sovereignty, right to live, and dignity. Our satellite that cleaves through space is the proud sign that unfolds the future of the most powerful state in the world." The same article, like many others, warns North Korea

<sup>22</sup> "North Korea May Have Tested Components of A Hydrogen Bomb" CNN, January 29, 2016; "North Korea Launches 'Satellite,' Sparks Fears About Long-Range Missile Program" Washington Post, February 6, 2016.

<sup>23</sup> Alex Lockie, "North Korea Threatens 'Nuclear Thunderbolts' as U.S. And China Finally Work Together" American Military News (April 14, 2017); Fox News, "U.S. General: North Korea 'Will' Develop Nuclear Capabilities to Hit America" (September 20, 2016) [www.foxnews.com/world/2016/09/20/north-korea-says-successfully-ground-tests-new-rocket-engine.html](http://www.foxnews.com/world/2016/09/20/north-korea-says-successfully-ground-tests-new-rocket-engine.html)

makes “constant preparations so that we can fire the nuclear warheads, which have been deployed for actual warfare for the sake of national defense, at any moment!”<sup>24</sup>

On April 30, 2017, South Korean officials told The Korea Times and YTN TV that North Korea’s test of a medium-range missile on April 29 was not a failure, as widely reported in the world press, because it was deliberately detonated at 72 kilometers altitude. [REDACTED]

[REDACTED] According to South Korean officials, “It’s believed the explosion was a test to develop a nuclear weapon different from existing ones.” Japan’s Tetsuro Kosaka wrote in Nikkei, “Pyongyang could be saying, ‘We could launch an electromagnetic pulse (EMP) attack if things get really ugly.’”<sup>25</sup>

On September 3, 2017, North Korea conducted its sixth underground nuclear test. The test produced a seismic signal of 6.3 on the Richter scale, indicating a yield of over 100 kilotons. Shortly after that test, North Korea released an article titled “Kim Jong Un Gives Guidance to Nuclear Weaponization,” which contained the following paragraph: **“The H-bomb, the explosive power of which is adjustable from tens kiloton to hundreds kiloton, is a multifunctional thermonuclear nuke with great destructive power which can be detonated even at high altitudes for super-powerful EMP attack according to strategic goals.”** On September 4, 2017, Pyongyang published a technical report “The EMP Might of Nuclear Weapons” accurately describing what the Russians and Chinese call a Super-EMP nuclear weapon. These warnings leave little room for wishful thinking by the U.S. leadership.<sup>26</sup>

---

<sup>24</sup> Rodong Sinmun (March 7, 2016).

<sup>25</sup> Tetsuro Kosaka, “North Korea’s ‘Failed’ Missile Test May Have Been a Thinly Disguised Threat,” Nikkei (May 2, 2017).

<sup>26</sup> Kim Song-won, “The EMP Might of Nuclear Weapons,” Rodong Sinmun, Pyongyang, (September 4, 2017).



## Non-Nuclear EMP Weapons

Terrorists, criminals, and even disgruntled individuals have already made localized EMP attacks using radio frequency weapons (RFWs) in Europe and Asia. Probably sooner rather than later, the RFW threat will come to America.

RFWs typically are much less powerful than nuclear weapons and much more localized in their effects, usually having a range of one kilometer or less. And unlike damage from guns and bombs, an attack by RFWs is much less conspicuous, and may even be misconstrued as an unusual accident arising from faulty components and systemic failure.

Some documented examples of successful attacks using Radio Frequency Weapons, and accidents involving electromagnetic transients, are described in the DoD *Pocket Guide for Security Procedures and Protocols for Mitigating Radio Frequency Threats*.<sup>27</sup>

For example, North Korea used a Radio Frequency Weapon, purchased from Russia, to attack airliners and impose an “electromagnetic blockade” on air traffic to Seoul, South Korea’s capitol. The repeated attacks by RFW also disrupted communications and the operation of automobiles in several South Korean cities in December 2010; March 9, 2011; and April-May 2012.<sup>28</sup>

---

<sup>27</sup> U.S. Department of Defense, “*Pocket Guide for Security Procedures and Protocols for Mitigating Radio Frequency Threats* (Technical Support Working Group, Directed Energy Technical Office, Dahlgren Naval Surface Warfare Center).

<sup>28</sup> “Massive GPS Jamming Attack by North Korea” GPSWORLD.COM (May 8, 2012).

## Physical Attacks on Power Grids

On April 16, 2013, parties unknown used AK-47s to attack the Metcalf transformer substation that services San Jose, the Silicon Valley, and is an important part of the Western Grid. Blackout of the Western Grid could impede U.S. power projection capabilities against North Korea.

Cases of physical sabotage of electric power grids include the following:

- On October 27, 2013, the Knights Templars, a terrorist drug cartel, used explosives and small arms to blackout Mexico's Michoacan State, putting 420,000 people into the dark, isolating them from federal police, so they could publicly assassinate town and village leaders opposed to the drug trade.
- On June 9, 2014, Al Qaeda in The Arabian Peninsula (AQAP) used rocket-propelled grenade launchers to attack powerline towers, blacking-out all of Yemen, a nation of 16 cities and 24 million people. It is the first time in history terrorists have blacked-out an entire nation.
- On January 25, 2015, the Taliban blacked-out most of the electric grid in Pakistan, a nuclear weapons state.

All of these blackouts were temporary, caused by sabotage of powerlines or small substations. A coordinated attack on a relatively small number of the most important transformer substations could cause a protracted blackout lasting months. The Wall Street Journal has reported that a study by the U.S. FERC concluded that a terrorist attack that destroys just 9 key transformer substations could cause a protracted nationwide blackout.<sup>29</sup>

---

<sup>29</sup> Pry, *Blackout Wars*, op. cit.; Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism" Wall Street Journal, February 5, 2014.

## Cyber-Attacks on Power Grids

Suspected and known cases of cyber-attacks causing blackouts of power grids include the following:

- On March 31, 2015, Turkey's national electric grid was temporarily blacked-out, briefly causing widespread chaos to businesses and society in a NATO member and crucial U.S. Middle Eastern ally. Reportedly, Iran caused the blackout by a cyber-attack. Weeks later, amidst a confrontation with Russia over shooting down a Russian jet that violated Turkish airspace, Turkey denied being victimized by an Iranian cyber-blackout. If Iran was the culprit, it would be the first time in history that a nationwide blackout resulted from cyber warfare.
- On December 23, 2015, a partial blackout of Ukraine's electric grid that lasted 1 to 6 hours, affecting 230,000 people, is widely regarded as the first confirmed case of a successful cyber-attack on an electric grid. The cyber-blackout is attributed to Russia.
- A year later, on December 17, 2016, Ukraine was again victimized, allegedly by Russians disrupting power grid control systems to temporarily blackout over 100 cities and towns.

Cyber-attacks, the use of computer viruses and hacking to invade and manipulate information and SCADA systems, is described by some U.S. political and military leaders as one of the greatest threats facing the United States. Every day, literally thousands of cyber-attacks are made on U.S. civilian and military systems, most of them designed to steal information.

Then Joint Chiefs Chairman, General Martin Dempsey, warned on June 27, 2013, that the United States must be prepared for the revolutionary threat represented by cyber warfare: "One thing is clear. Cyber has escalated from an issue of moderate concern to one of the most serious threats to our national security," cautioned Chairman Dempsey, "We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse."<sup>30</sup>

On July 6, 2014, reports surfaced that Russian intelligence services allegedly infected 1,000 power plants in Western Europe and the United States with a new computer virus called Dragonfly. No one has stated what Dragonfly is supposed to do. Some analysts think it was just probing the defenses of western electric grids. Others think Dragonfly may have inserted logic bombs into SCADA systems that can disrupt the operation of electric power plants in a future crisis.

Tomorrow's cyber super-threat, that with computer viruses and hacking alone can blackout the national electric grid for a year or more, may already be upon us today.

---

<sup>30</sup> Claudette Roulo, *DoD News*, Armed Force Press Service, June 27, 2013.

Admiral Michael Rogers on November 20, 2014, warned the House Permanent Select Committee on Intelligence that sophisticated great powers like China and Russia have the capability to blackout the entire U.S. national electric grid for months or years by means of cyber-attack, according to press reports. Admiral Rogers, as Chief of U.S. Cyber Command and Director of the National Security Agency, is officially the foremost U.S. authority on the cyber threat. “It is only a matter of the when, not if, that we are going to see something traumatic,” Admiral Rogers testified to Congress.<sup>31</sup>

In June 2015, congressional hearings revealed the discovery, about a year earlier, that China, probably the Chinese People’s Liberation Army (PLA), hacked into computer files at the U.S. Office of Personnel Management and stole sensitive information on 30 million federal employees and U.S. citizens.

Russia apparently made a cyber-attack on the U.S. Joint Chiefs of Staff in July 2015 that crippled an unclassified e-mail communications network used by the Joint Chiefs. “The U.S. military believes hackers connected to Russia are behind the recent intrusion into a key, unclassified e-mail server used by the office of the Joint Chiefs,” according to press reports, “Military officials assessed the attack had a sophistication that indicates it came from a state-associated actor.” The widely reported Russian cyber-attack on the Joint Chiefs disrupted e-mail communications for 4,000 users at the Defense Department for over 10 days.<sup>32</sup>

In April 2015, another Russian cyber-attack reportedly penetrated “sensitive parts of the White House computer system.”<sup>33</sup>

Few Americans make any connection between cyber-thefts and intrusions, such as those described above, and EMP attacks on the grid that could threaten the existence of society. But in the context of foreign military doctrine on Information Warfare, these cyber-thefts and intrusions look less like isolated cases of hacking and more like systematic probing of U.S. defenses and gauging Washington’s reactions—perhaps in preparation for an all-out cyber offensive that would include physical sabotage, radiofrequency weapons, and nuclear EMP attack. In Nazi Germany’s blitzkrieg strategy, the massed onslaught of heavy armored divisions was preceded by scouting and probing by their motorcycle corps. The same principle may be at work here in cyber space with probing attacks on the U.S. from China, Russia, North Korea and Iran.

---

<sup>31</sup> CNN November 21, 2014. However, Jonathan Pollett, a cyber-security expert, in an article challenged Admiral Rogers’ warning as wrong, or misunderstood and exaggerated by the press: “No, hackers can’t take down the entire, or even a widespread portion of the U.S. electric grid. From a logistical standpoint, this would be far too difficult to realistically pull off,” writes Pollett in “What Hackers Can Do To Our Power Grid,” Business Insider (November 23, 2014).

<sup>32</sup> CNN, “Official: Russia Suspected In Joint Chiefs E-mail Server Intrusion,” August 7, 2015.

<sup>33</sup> Ibid.

### *All Hazards Strategy*

We recommend an “all hazards” strategy to protect the nation by addressing the worst threat—nuclear EMP attack. Nuclear EMP is worse than natural EMP because it combines several threats in one. Nuclear EMP has a long-wavelength component like a geomagnetic super-storm, a short-wavelength component like Radio-Frequency Weapons, a mid-wavelength component like lightning—and is potentially more widespread and can do more damage than all three. Measures to protect electric grids and other critical infrastructures from EMP can also be designed to make these systems more resilient against cyber-attacks, sabotage, and severe weather.

A U.S. Army War College Study, *“In The Dark: Planning for a Catastrophic Critical Infrastructure Event,”* (2011) warned U.S. Cyber Command that U.S. doctrine should not overly focus on computer viruses to the exclusion of EMP attack and the full spectrum of other threats, as planned by potential adversaries.

Reinforcing the above, a Russian technical article on cyber warfare notes that a cyber-attack can collapse “the system of state and military control...its military and economic infrastructure” because of “electromagnetic weapons...an electromagnetic pulse acts on an object through wire leads on infrastructure, including telephone lines, cables, external power supply and output of information.”<sup>34</sup>

*Resilient Military Systems and the Advanced Cyber Threat*, a January 2013 study by the Defense Science Board, recommends that it may be necessary for the U.S. to respond to an all-out cyber warfare operation with nuclear deterrence—or nuclear war. The Defense Science Board warns that while operationally “a nuclear and cyber-attack are very different” in terms of the consequences “the existential impact to the United States is the same.”

The Defense Science Board likewise warns that cyber warfare is not only about computer viruses and hacking, but becomes an existential threat “from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities (a “full spectrum” adversary).”

---

<sup>34</sup> Maxim Shepovalenko, *Military-Industrial Courier* (July 3, 2013).



## Misinformation about EMP and the North Korean Threat

EMP non-experts often dismiss the possibility of a nuclear EMP attack from North Korea as “science fiction” and “unlikely” because either they lack knowledge of the effects of the Soviet and U.S. high altitude nuclear tests in the early 1960s, do not have access to or understand the extensive body of testing and analysis carried out by the DoD over the last fifty-five years, or they mistakenly believe the nuclear weapons currently possessed by North Korea are incapable of making an effective EMP attack.

One EMP skeptic correctly implies in his article that it is analytically risky to draw conclusions about the EMP threat when so much of the data is classified. It is riskier still for analysts with no technical training on EMP and without working professionally in the defense or intelligence communities on the EMP threat, to conclude the EMP threat is not real—dismissing the consensus view of EMP experts who have advanced degrees in physics and electrical engineering, have worked on EMP generation and effects for several decades, have throughout that time had access to classified data, and have conducted simulated EMP tests on a wide variety of electronic systems, beginning in 1963.

I offer this commentary to correct errors of fact, analysis, and myths about EMP and the threat from North Korea:

- Even primitive, low-yield nuclear weapons are such a significant EMP threat that rogue states or terrorists may well prefer using a nuclear weapon for EMP attack, instead of destroying a city: “Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack.”<sup>35</sup>
- North Korea may either now or in the future be armed with what the Russians call “Super-EMP” weapons, that can generate extraordinarily high-intensity EMP fields, according to unclassified Russian sources up to 200,000 volts per meter.<sup>36</sup> In 2004, two Russian generals, both EMP experts, warned the EMP Commission that the design for Russia’s Super-EMP warhead was “accidentally” transferred to North Korea, and that due to “brain drain” Russian scientists were in North Korea, helping with their missile and nuclear weapon programs. South Korean military intelligence told their press that Russian scientists are in North Korea helping develop an EMP nuclear weapon. In 2013, a People’s Republic of China military commentator stated North Korea has Super-EMP nuclear weapons. The EMP Commission 2004 Report warns: “Certain types of relatively

---

<sup>35</sup> EMP Commission *Executive Report 2004*, p. 2.

<sup>36</sup> “Russia: Nuclear Response To America Is Possible Using Super-EMP Factor,” Aleksey Vaschenko, “A Nuclear Response To America Is Possible” *Zavtra* (November 1, 2006).

low-yield nuclear weapons can be employed to generate potentially catastrophic EMP effects over wide geographic areas, and designs for variants of such weapons may have been illicitly trafficked for a quarter-century.”<sup>37</sup>

- Super-EMP weapons are low-yield and designed to produce not a big kinetic explosion, but rather a high level of gamma rays, which is what generates the high-frequency E1 EMP most damaging to the broadest range of electronics. North Korean nuclear tests, including the first in 2006, whose occurrence was predicted to the EMP Commission two years in advance and by the two Russian EMP experts, are consistent with testing of a Super-EMP weapon.
- The design of a Super-EMP weapon could be relatively small and lightweight. Such a device could fit inside North Korea’s satellites that can orbit over the United States. [REDACTED]  
[REDACTED], resembling a Russian secret weapon developed during the Cold War that could have used a nuclear-armed satellite to make a surprise EMP attack on the United States.
- One popular myth is that during the 1962 STARFISH PRIME high-altitude nuclear test “just one string of street lights failed in Honolulu” and that the test proves EMP is no threat. In fact, the EMP knocked-out thirty-six strings of street lights, caused a telecommunications microwave relay station to fail, burned out high-frequency radio links, set off burglar alarms, and caused other damage. The Hawaiian Islands did not experience a catastrophic protracted blackout because they were on the far edge of the EMP field contour, where effects are weakest, and were still in an age dominated by vacuum tube electronics. In addition, the slow pulse (E3) component of the EMP waveform couples most effectively to very long electric power transmission lines present on large land masses but not present in Hawaii. A 1983 twelve-page report, formerly classified Confidential Restricted Data, summarizing the observed EMP effects of the Fishbowl U.S. exo-atmospheric tests, has recently been reviewed at the request of the EMP Commission and found to be unclassified, but has been placed under a distribution restriction by the Department of Defense that makes it unavailable to analysts and others concerned about the viability of U.S. critical national infrastructure. No justification for the distribution restriction has been given.
- Russia in 1961-62 conducted a series of high-altitude EMP tests over Kazakhstan, an industrialized area nearly as large as Western Europe, that damaged the Kazakh electric grid. Modern electronics are much more vulnerable to EMP than the electronics of 1962 exposed to STARFISH PRIME and the Kazakh nuclear tests. A similar EMP event over the U.S. today would be an existential threat to our society, due to our dependence on the

<sup>37</sup> EMP Commission *Executive Report 2004*, p. 2. Kim Min-sek and Yoo Jee-ho, “Military Source Warns of North’s EMP Bomb” JoonAng Daily (September 2, 2009). Li Daguang, “North Korea Electromagnetic Attack Threatens South Korea’s Information Warfare Capabilities” Tzu Chin, No. 260 (Hong Kong: June 1, 2012), in “PRC Owned HK Journal Says DPRK May Build EMP Bombs To Paralyze ROK Weapons System.”

electric power grid and other lifeline infrastructures, all the more susceptible due to the vulnerability of advanced electronic controls and communications.

- One popular but poorly informed author mistakenly inferred from a single simulated EMP test series on vehicles that, because only 6 of 55 vehicles were shut down, vehicle transportation would continue after an EMP event. During that test one of the vehicles was damaged and could not be operated until repaired, indicating that at least 2 percent of vehicles would be at risk of EMP damage. Even a 2 percent failure rate of vehicles would cause traffic jams, crippling transportation in urban areas. Moreover, the EMP test protocol limited testing vehicles only to upset, not to damage, because the EMP Commission could not afford to repair damaged cars; however, one vehicle was damaged by EMP despite best efforts to limit the effects to upset. Several of the vehicles tested stopped operating but could be restarted. Over 50 years of EMP testing indicates that full field damage to vehicles would probably be much higher than was observed on the limited tests. Today's vehicles depend on a much larger complement of electronics than the vehicles tested by the Commission more than a decade ago. Furthermore, vehicles cannot run without fuel, which cannot be pumped in a protracted electrical blackout.
- Another poorly informed analyst wondered why EMP from atmospheric nuclear tests in Nevada did not blackout Las Vegas. The nuclear tests he describes were all endo-atmospheric tests that do not generate appreciable EMP fields beyond a range of about 5 miles. The HEMP threat of interest requires exo-atmospheric detonation, at 30 kilometers altitude or above, and produces EMP out to ranges of hundreds to thousands of miles, depending on the height of detonation. Las Vegas was not affected by EMP because those endo-atmospheric nuclear tests generated much lower level fields outside the Nevada Test Site.
- Another poorly informed author miscalculates that "a 20-kiloton bomb detonated at optimum height would have a maximum EMP damage distance of 20 kilometers" in part because he mistakenly assumes "15,000 volts/meter or higher" in the E1 EMP extends only a short distance from the detonation point and that field strength is necessary for damage. These figures are extreme underestimates of the EMP field range and an extreme overestimate of system damage field thresholds. A one meter wire connected to a semiconductor device, such as a mouse cord or interconnection cable, would place hundreds to thousands of volts on microelectronic devices out to ranges of hundreds of miles for low-yield exo-atmospheric detonations. Semiconductor junctions operate at a few volts, and will experience breakdown at a few volts over their operating point, then allowing their power supply to destroy junctions experiencing reverse bias breakdown, as has been our experience in many EMP tests.
- The North Korean missile test on April 29, 2017, that apparently either failed or deliberately detonated at an altitude of 72 kilometers [REDACTED] [REDACTED] could have been a test for creating a potentially damaging EMP field to a distance, not of one ill-informed author's miscalculated 20

kilometers, but of about 930 kilometers [Kilometers Radius = 110 (Kilometers Burst Height to the 0.5 Power)].

- Ill-informed authors often mistakenly ignore system upset as a vulnerability. Digital electronics can be upset by extraneous pulses of a few volts. For unmanned control systems present within the electric power grid, long-haul communication repeater stations, and gas pipelines, an electronic upset can be tantamount to permanent damage. Temporary upset of electronics can also have catastrophic consequences for military operations. No electronics should be considered invulnerable to EMP unless hardened or tested to certify survivability. Some highly critical unprotected electronics have been upset or damaged in simulated EMP tests, not at one author's alleged "15,000 volts/meter or higher" but at threat levels far below 1,000 volts/meter.

Therefore, even for a low-yield 10 to 20 kiloton weapon, the EMP field should be considered dangerous for unprotected U.S. systems. The EMP Commission 2004 Report warned against the U.S. military's increasing use of commercial-off-the-shelf-technology that is not protected against EMP: "Our increasing dependence on advanced electronics systems results in the potential for an increased EMP vulnerability of our technologically advanced forces, and if unaddressed makes EMP employment by an adversary an attractive asymmetric option."<sup>38</sup>

---

<sup>38</sup> EMP Commission *Executive Report 2004*, p. 47.

## North Korea Nuclear EMP Attack: An Existential Threat

While most military and other analysts are fixated on when in the future North Korea will develop highly reliable intercontinental missiles, guidance systems, and reentry vehicles capable of striking a U.S. city, the present and continuing threat from EMP is largely ignored. EMP attack does not require an accurate guidance system because the area of effect, having a radius of hundreds or thousands of kilometers, is so large. No reentry vehicle is needed because the warhead is detonated at high-altitude, above the atmosphere. Missile reliability matters little because only one missile has to work to make an EMP attack against an entire nation.

North Korea could make an EMP attack against the United States by ICBM, or by launching a short-range missile off a freighter or submarine or by lofting a warhead to 30 kilometers burst height by balloon. While such lower-altitude EMP attacks would not cover the whole U.S. mainland, as would an attack at higher-altitude (300 kilometers), even a balloon-lofted warhead detonated at 30 kilometers altitude could blackout the Eastern Grid that supports most of the population and generates 75 percent of U.S. electricity.

An EMP attack could also be made by a North Korean satellite.

North Korea's KMS-3 and KMS-4 satellites were launched to the south on polar trajectories and passed over the United States on their first orbit. Pyongyang launched KMS-4 on February 7, 2017, shortly after its fourth illegal nuclear test on January 6, 2017, that began the present protracted nuclear crisis with Pyongyang.

[REDACTED]  
[REDACTED], resembling a Russian secret weapon developed during the Cold War, called the Fractional Orbital Bombardment System (FOBS) that would have used a nuclear-armed satellite to make a surprise EMP attack on the United States.<sup>39</sup>

Ambassador Henry Cooper, former Director of the U.S. Strategic Defense Initiative, and a preeminent expert on missile defenses and space weapons, has written numerous articles warning about the potential North Korean EMP threat from their satellites. For example, on September 20, 2016 Ambassador Cooper wrote:

*U.S. ballistic missile defense (BMD) interceptors are designed to intercept a few North Korean ICBMs that approach the United States over the North Polar region. But current U.S. BMD systems are not arranged to defend against even a single ICBM that approaches the United States from over the South Polar region, which is the direction toward which North Korea launches its*

---

<sup>39</sup> Miroslav Gyurosi, *The Soviet Fractional Orbital Bombardment System Program*, (January 2010) Technical Report APA-TR-2010-010.



*satellites...This is not a new idea. The Soviets pioneered and tested just such a specific capability decades ago—we call it a Fractional Orbital Bombardment System (FOBS)...So, North Korea doesn't need an ICBM to create this existential threat. It could use its demonstrated satellite launcher to carry a nuclear weapon over the South Polar region and detonate it...over the United States to create a high-altitude electromagnetic pulse (HEMP)...The result could be to shut down the U.S. electric power grid for an indefinite period, leading to the death within a year of up to 90 percent of all Americans—as the EMP Commission testified over eight years ago.*<sup>40</sup>

Former NASA rocket scientist James Oberger visited North Korea's Sohae space launch base, witnessed elaborate measures undertaken to conceal space launch payloads, and concludes in a 2017 article that the EMP threat from North Korea's satellites should be taken seriously:

*...there have been fears expressed that North Korea might use a satellite to carry a small nuclear warhead into orbit and then detonate it over the United States for an EMP strike. These concerns seem extreme and require an astronomical scale of irrationality on the part of the regime. The most frightening aspect, I've come to realize, is that exactly such a scale of insanity is now evident in the rest of their "space program." That doomsday scenario, it now seems, has been plausible enough to compel the United States to take active measures to ensure that no North Korean satellite, unless thoroughly inspected before launch, be allowed to reach orbit and ever overfly the United States.*<sup>41</sup>

An earlier generation immediately understood the alarming strategic significance of Sputnik in 1957, yet few today understand the strategic significance of North Korea's satellites, perhaps because of widespread ignorance about EMP.

---

<sup>40</sup> Ambassador Henry F. Cooper, "Whistling Past The Graveyard..." High Frontier (September 20, 2016) [highfrontier.org/sept-20-2016-whistling-past-the-graveyard](http://highfrontier.org/sept-20-2016-whistling-past-the-graveyard). See also: [highfrontier.org/category/fobs](http://highfrontier.org/category/fobs). On up to 90 percent U.S. fatalities from an EMP attack, see: U.S. House of Representatives, Hearing, "Threat Posed by Electromagnetic Pulse (EMP) Attack" Committee on Armed Services (Washington, D.C.: July 10, 2008), p. 9.

<sup>41</sup> Jim Oberger, Space Review (February 6, 2017) [www.thespacereview.com/article/3164/1](http://www.thespacereview.com/article/3164/1)

## The Fragility of Complex Systems

When assessing the potential vulnerability of U.S. military forces and civilian critical infrastructures to EMP, it is necessary to be mindful of the complex interdependencies of these highly-networked systems, such that EMP upset and damage of a very small fraction of the total system can cause total system failure.

Real world failures of electric grids from various causes indicate that a nuclear EMP attack would have catastrophic consequences. Significant and highly disruptive blackouts have been caused by single-point failures cascading into system-wide failures, originating from damage comprising far less than 1 percent of the total system. For example:

- The Great Northeast Blackout of 2003—that put 50 million people in the dark for a day, contributed to at least 11 deaths, and cost an estimated \$6 billion—originated from a single failure point when a powerline contacted a tree branch, damaging less than 0.0000001 (0.00001 percent) of the system.
- The New York City Blackout of 1977, that resulted in the arrest of 4,500 looters and injury of 550 police officers, was caused by a lightning strike on a substation that tripped two circuit breakers.
- The Great Northeast Blackout of 1965, that affected 30 million people, happened because a protective relay on a transmission line was improperly set.
- India’s nationwide blackout of July 30-31, 2012—the largest blackout in history, affecting 670 million people, 9 percent of the world population—was caused by overload of a single high-voltage powerline.
- India’s blackout of January 2, 2001—affecting 226 million people—was caused by equipment failure at the Uttar Pradesh substation.
- Indonesia’s blackout of August 18, 2005—affecting 100 million people—was caused by overload of a high-voltage powerline.
- Brazil’s blackout of March 11, 1999—affecting 97 million people—was caused by a lightning strike on an EHV transformer substation.
- Italy’s blackout of September 28, 2003—affecting 55 million people—was caused by overload of two high-voltage powerlines.
- Germany, France, Italy, and Spain experienced partial blackouts on November 4, 2006—affecting 10 to 15 million people—from accidental shutdown of a high-voltage powerline.
- The San Francisco blackout in April 2017 was caused by the failure of a single high voltage breaker at a substation.

In contrast to the above blackouts caused by single-point or small-scale failures, a nuclear EMP attack would inflict massive widespread damage to the electric grid causing a large number of

failure points. With few exceptions, the U.S. national electric grid is unhardened and untested against nuclear EMP attack.

In the event of a nuclear EMP attack on the United States, a widespread protracted blackout is inevitable. This commonsense assessment is also supported by the nation's best computer modeling:

Modeling by the U.S. FERC reportedly assesses that a terrorist attack that destroys just 9 EHV transformer substations would produce catastrophic damage, causing a protracted nationwide blackout.

Modeling by the EMP Commission assesses that a terrorist nuclear EMP attack, using a primitive 10-kiloton nuclear weapon, could destroy many EHV transformers and thousands of SCADA and electronic systems, causing catastrophic collapse and protracted blackout of the U.S. power grids, putting at risk the lives of millions.

For the best unclassified modeling assessments of likely damage to the U.S. national electric grid from nuclear EMP attack see the following: U.S. FERC Interagency Report, coordinated with the DoD and Oak Ridge National Laboratory: *Electromagnetic Pulse: Effects on the U.S. Power Grid, Executive Summary* (2010); U.S. FERC Interagency Report by Edward Savage, James Gilbert and William Radasky, *The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid* (Meta-R-320) Metatech Corporation (January 2010); U.S. FERC Interagency Report by James Gilbert, John Kappenman, William Radasky, and Edward Savage, *The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid* (Meta-R-321) Metatech Corporation (January 2010).

## **Regulatory Failures by the U.S. Federal Energy Regulatory Commission, the North American Energy Regulatory Corporation, and the Electric Power Industry**

The current largely self-regulatory structure of the U.S. Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the electric power industry was not designed to address U.S. survival under nuclear EMP or other hostile attack. The Commission assesses that the existing regulatory framework for safeguarding the security and reliability of the electric power grid, which is based upon a partnership between the U.S. FERC and the private NERC representing the utilities, is not able to protect the U.S. against hostile attack. The U.S. FERC and NERC standards for protecting the power grids from geomagnetic disturbances caused by solar storms are also inadequate to address storms of historical record.<sup>42</sup>

The U.S. FERC, the U.S. government agency that is supposed to partner with NERC in protecting the national electric grid, has publicly testified before Congress that the U.S. FERC lacks regulatory power to compel NERC and the electric power industry to protect the grid from natural and nuclear EMP and other threats.

Consider the contrast in regulatory authority between the U.S. FERC and, as examples, the U.S. Nuclear Regulatory Commission (NRC), the U.S. Federal Aviation Administration (FAA), the U.S. Department of Transportation (DOT), or the U.S. Food and Drug Administration (FDA):

- The NRC has regulatory power to compel the nuclear power industry to incorporate nuclear reactor design features to make nuclear power safe. (To date, however, the NRC has not incorporated EMP survival criteria into its regulations. By the NRC's failure to use its authority to mandate protection from EMP of U.S. nuclear reactor control, safe shutdown, cooling, and other reactor systems and spent fuel storage systems, the NRC continues to place at risk the safety and survivability of the 99 U.S. commercial power reactors in operation and the safety of the people living in the vicinity of these reactors.)
- The FAA has regulatory power to compel the airlines industry to ground aircraft considered unsafe, to change aircraft operating procedures considered unsafe, and to make repairs or improvements to aircraft in order to protect the lives of passengers.
- The DOT has regulatory power to compel the automobile industry to install on cars safety glass, seatbelts, and airbags in order to protect the lives of the driving public.

---

<sup>42</sup> John G. Kappenman and Dr. William Radasky, *Examination of NERC GMD Standards and Validation of Ground Models and Geo-Electric Fields* (Storm Analysis Consultants and Metatech Corporation, July 30, 2014) adopted as an EMP Commission Staff Paper. See also Foundation for Resilient Societies, Comments Submitted on Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events, U.S. FERC Docket No. RM15-11-000, July 27, 2015; supplementary comments submitted August 10, 2015.

### *Underestimating the EMP Threat to Transformers*

The most recent example of industry inadequacy as a champion for EMP preparedness is a study by EPRI that purports to prove a nuclear EMP attack would destroy few, if any EHV transformers. I have reviewed this study and find many flaws in the EPRI assessment. Contrary to EPRI, many EHV transformers would be at risk from the same nuclear EMP attack postulated by EPRI. The EMP Commission has produced a report providing a more realistic assessment of the E3 EMP field strengths likely to be generated by a nuclear EMP attack. The Commission's unclassified assessment of the E3 EMP threat should better inform the electric power industry and other private sector critical infrastructures so they can better protect themselves. See the EMP Commission Report by Dr. Edward B. Savage and Dr. William A. Radasky, *Development of Estimates of Peak Values of the Late-Time (E3) HEMP Heave Electric Fields Using Measured Data from High Altitude Nuclear Testing* (Metatech: Meta-R-440, July 10, 2017).

- The FDA has power to regulate the quality of food and drugs, and can ban under criminal penalty the sale of products deemed by the FDA to be unsafe to the public.

Unlike the NRC, FAA, DOT, FDA or any other U.S. government regulatory agency, the U.S. FERC does not have legal authority to compel the industry it is supposed to regulate to act in the public interest. For example, the U.S. FERC lacks legal power to direct NERC and the electric utilities to install devices to protect the grid.

Currently, the U.S. FERC only has the power to ask NERC to propose a Standard to protect the grid. NERC standards are approved, or rejected, by its membership, which is largely made up of representatives from the electric power industry. Once NERC proposes a Standard to the U.S. FERC, the FERC cannot modify the Standard, but must accept or reject the proposed Standard. If the U.S. FERC rejects the proposed Standard, NERC goes back to the drawing board, and the process starts all over again.

The geomagnetic disturbance standards proposed by the NERC that the U.S. FERC has adopted to date substantially underestimate the problem, and no standards for protecting the grid against nuclear or non-nuclear EMP weapons have been proposed or adopted.

Regulatory inadequacy over the electric power industry for national security is demonstrated, not only in the failure of industry to protect the grid, but in lobbying by NERC, EPRI, EEI and other industry groups to oppose initiatives by federal and state officials and private citizens to protect the grid from EMP over the past 9 years by implementing the recommendations of the EMP Commission made in 2008. Texas State Senator Bob Hall speaks for many Americans frustrated by the electric power industry's active, and frequently misleading, opposition:

*As a Texas State Senator who tried in the 2015 legislative session to get a bill passed to harden the Texas grid against an EMP attack or nature's GMD, I*



*learned first-hand the strong control the electric power company lobby has on elected officials. We did manage to get a weak bill passed in the Senate but the power companies had it killed in the House. A very deceitful document which was carefully designed to mislead legislators was provided by the power company lobbyist to legislators at a critical moment in the process. The document was not just misleading, it actually contained false statements. The EMP/GMD threat is real and it is not “if” but WHEN it will happen. The responsibility for the catastrophic destruction and wide spread death of Americans which will occur will be on the hands of the executives of the power companies because they know what needs to be done and are refusing to do it. In my opinion power company executives, by refusing to work with the legislature to protect the electrical grid infrastructure are committing an egregious act that is equivalent to treason. I know and understand what I am saying. As a young U.S. Air Force captain, with a degree in electrical engineering from The Citadel, I was the project officer who lead the Air Force/contractor team which designed, developed and installed the modification to “harden” the Minuteman strategic missile to protect it from an EMP attack. The American people must demand that the power company executives that are hiding the truth stop deceiving the people and immediately begin protecting our electrical grid so that life as we know it today will not end when the terrorist EMP attack comes.*

In March 2016, the U.S. GAO published a report with the (misleading) title *Critical Infrastructure Protection: Federal Agencies Have Taken Actions to Address Electromagnetic Risks, But Opportunities Exist to Further Assess Risks and Strengthen Collaboration* (GAO-16-243). Appendices in the U.S. GAO report reveal that none of the essential measures recommended by the EMP Commission to protect the national electric grid have been undertaken:

<b><u>Recommendation</u></b>	<b><u>Action</u></b>
Expand and extend emergency power supplies .....	None
Extend black start capability .....	None
Prioritize and protect critical nodes .....	None
Expand and assure intelligent islanding capability .....	None
Assure protection of high-value generation assets.....	None
Assure protection of high-value transmission assets .....	None
Assure sufficient numbers of adequately trained recovery personnel ..	None

In the U.S. GAO report, the “actions” undertaken by federal agencies to address EMP are almost entirely studies and a few experimental programs.

During a hearing before the Senate Homeland Security and Government Affairs Committee (SHSGA) on July 22, 2015, under questioning by the Chairman, Senator Ron Johnson, the U.S.

GAO acknowledged that none of the recommendations of the EMP Commission to protect the national grid from EMP have been implemented by the U.S. Department of Homeland Security, U.S. Department of Energy, U.S. FERC, or NERC.

The U.S. GAO report explained lack of progress in protecting the national electric grid from EMP as due to a lack of leadership, because no one was in charge of solving the EMP problem: “DHS and DOE, in conjunction with industry, have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks.”

## **The 2014 Intelligence Report**

The report by the Joint Atomic Energy Intelligence Committee (JAEIC) on EMP issued in 2014 is factually erroneous and analytically unsound. I recommend that the Director of National Intelligence withdraw the JAEIC EMP Report and direct that the EMP Commission critique of the JAEIC EMP Report be circulated to all the recipients of the 2014 JAEIC EMP Report, which is a threat to national security by impeding progress on EMP understanding and protection.

## Conclusions

The United States critical national infrastructure faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade EMP attack, and natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about a high altitude nuclear-weapon generated EMP attack as a tactic by which the Soviet Union could suppress the ability of the U.S. national command authority and U.S. strategic forces to respond to a nuclear attack, and thus destroy the U.S. deterrence provided by assured nuclear retaliation. Within the last decade, newly nuclear-armed adversaries, including North Korea, have been developing the ability and threatening to carry out an EMP attack against the U.S. Such an attack would give countries that have only a small number of nuclear weapons the ability to cause widespread, long-lasting damage to U.S. critical national infrastructures, to the United States itself as a viable country, and to the survival of a majority of its population.

While during the Cold War major efforts were undertaken by the DoD to assure that the U.S. national command authority and U.S. strategic forces could survive and operate after an EMP attack, no major efforts were then thought necessary by the national leadership to protect critical national infrastructures, provided that nuclear deterrence was successful. With the development of small nuclear arsenals and long-range missiles by small, hostile, potentially unstable and irrational countries, including North Korea, the threat of a nuclear EMP attack against the U.S. becomes one of the few ways that such a country could inflict devastating damage to the U.S. Therefore, it is urgent that the U.S. national leadership address the EMP threat as a critical, existential issue, and give a high priority to assuring the necessary leadership is engaged and the necessary steps are taken to protect the country from EMP. Otherwise, foreign adversaries may reasonably consider such an attack as one which can gravely damage the U.S. by striking at its technological Achilles' heel, without having to overcome the U.S. military.

Protecting and defending the national electric grid and other critical infrastructures from EMP attack could be accomplished at reasonable cost and minimal disruption to the present systems that comprise our critical infrastructure; all commensurate with Trump Administration plans to repair and improve U.S. infrastructures, increase their reliability, and strengthen our homeland defense and military capability. Continued failure to address our country's vulnerability to high altitude nuclear weapon-generated EMP invites attack.

From: [Paul Stockton](#)  
To: [Paul Stockton](#); [Joseph McClelland](#)  
Subject: Draft Study  
Date: Thursday, April 26, 2018 4:23:26 PM  
Attachments: [APL GSE Study Sections I-IV April 26 2018.docx](#)

---

Joe, I hope you and your family are doing great! About a gazillion years ago, you/FERC hosted me for a brainstorming session on how to make use of the FAST Act emergency authorities. I have completed a draft at long last. Can you please murderize it, and share it with any colleagues who might offer comments by May 2?

Best, Paul

**Paul Stockton**

**Managing Director, Sonecon, LLC**

**325 7<sup>th</sup> Street NW**

**Suite 250**

**Washington, D.C. 20004**

**202-393-2228**

**Cell: 703 945 6574**

**pstockton@sonecon.com**



*DRAFT: NOT FOR USE OR CITATION  
WITHOUT PERMISSION OF THE AUTHOR*

# **RESILIENCE FOR GRID SECURITY EMERGENCIES: OPPORTUNITIES FOR INDUSTRY-GOVERNMENT COLLABORATION**

Paul N. Stockton (pstockton@sonecon.com)  
Report for the Johns Hopkins University Applied Physics Laboratory (APL)  
April 26, 2018

## **EXECUTIVE SUMMARY**

The United States Congress has opened the door to novel strategies for defending the U.S. electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act in December 2015, Congress granted the Secretary of Energy vast new authorities to use when the President declares that a grid security emergency exists. Most important, legislators authorized the Secretary of Energy to issue emergency orders to grid owners and operators to protect and restore grid reliability when attacks on their systems are imminent or underway.<sup>1</sup> The Federal Power Act is silent, however, on what the Secretary might order these owners and operators to do and how emergency orders can effectively bolster their protection efforts.

The onslaught of an attack would be the worst possible time to develop such orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid which could then be adjusted to fit the specific circumstances of an attack. Developing such orders in advance would help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. In turn, those contingency plans could provide the basis for training and exercise initiatives to prepare for the attacks to come.

This study is structured help the electricity subsector partner with the Department of Energy (DOE) to develop emergency orders and meet the broader policy and operational challenges that grid security emergencies will entail. In particular, the study examines how these partners might develop emergency orders to protect grid reliability against potentially catastrophic cyber and physical attacks, and – if major blackouts occur – help utilities accelerate the restoration of power.

---

<sup>1</sup> The "Fixing America's Surface Transportation Act" [hereinafter referred to as the FAST Act], Public Law 114-94, *U.S. Statutes at Large* 129 (2015): pp. 1773-4, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

DOE and their industry partners should develop emergency orders for three possible phases of grid security emergencies. The Federal Power Act specifies that the President can declare a grid security emergency (GSE) when there is “imminent danger” of an attack on electric infrastructure critical for national defense, economic security, and public health and safety. Strong foundations already exist for developing emergency orders for this initial, pre-attack phase of GSEs. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions, such as staffing up emergency operations centers, increasing available generation to help manage grid instabilities, and taking other precautionary measures.

Determining that a cyber or physical attack is imminent could be vastly more difficult than doing so for hurricanes. However, if the United States has sufficient warning of an attack, many of the same measures used to bolster preparedness against natural hazards might be adapted to provide pre-attack options for conservative operations. Promising opportunities also exist to develop measures tailored for cyber or physical threats. Emergency orders for conservative operations constitute “low hanging fruit;” industry and government partners should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The Federal Power Act also states that the President can declare a GSE when attacks are “occurring.” Industry and government partners should develop a second set of orders to use once attacks are underway, both to prevent power failures from cascading across the United States and to sustain electric service to major regional hospitals and other critical facilities. Existing electric industry plans and capabilities provide a strong basis to develop such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Emergency orders for equivalent *extraordinary measures* could provide useful “arrows in the quiver” in grid security emergencies, and could help integrate national security priorities into existing utility plans to counter grid instabilities.

A third set of potential emergency orders would help utilities accelerate power restoration if blackouts occur. Attacks that damage or destroy large number of high voltage transformers or other difficult-to-replace equipment could create outages that darken major portions of the United States for many weeks or even months. Power companies and DOE already have initiatives underway to meet this challenge. They should also collaborate to develop emergency orders to *accelerate restoration*. In particular, orders might be drafted to account for the risk that adversaries will continue attacking after their initial salvo, and launch follow-on strikes to disrupt restoration operations and lengthen U.S. power outages.

Of course, Russia, China, and other potential adversaries will not strike the grid merely to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to U.S. Defense installations, ports, and other civilian infrastructure essential for deploying and sustaining forces to the region. Emergency orders can be designed to help deter – and, if necessary, defeat – such attacks. This study proposes specific

options to do so, in support of the *National Security Strategy of the United States of America* and other sources of U.S. policy guidance.

The study also identifies ways that government and industry can pre-plan to communicate with the American people if adversaries strike. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks – and, potentially, attack the phone and internet-based communications systems on which utilities typically use coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications “playbooks” to prepare for grid security emergencies, and make doing so a core component of the emergency order development process.

These partners should also pre-plan to take advantage of an especially valuable way in which Congress amended the Federal Power Act: the creation of new provisions for emergency regulatory waivers and cost recovery for power companies. Legislators recognized that to comply with emergency orders, grid owners and operators might have to violate environmental regulations and other standards. The Act now protects entities from the enforcement of such violations if they occur as the result of complying with emergency orders. The FPA also provides for the recovery of costs that companies will incur in implementing those orders. This study suggests additional measures that industry and government may want to consider to facilitate compliance and reinforce the “value added” of emergency orders for countering attacks on the grid.

In addition, government and industry partners should examine the triggers and thresholds for declaring grid security emergencies and issuing emergency orders. Major ambiguities surround the criteria for making such declarations, especially for attacks that may be imminent. One option to clarify these criteria would be to leverage the electric industry’s focus on preserving “adequate levels of reliability,” and declare emergencies when adversaries are poised to create cascading power failures and other major disruptions across multiple states. However, the President should also retain the flexibility to declare GSEs for a broad range of other contingencies.

Industry and government partners should also identify opportunities to build broader resilience for grid security emergencies. Intensive follow-on work will be required to finalize the development of emergency orders and build utility-specific contingency plans to implement them in ways that account for accelerating structural changes in the electricity subsector (including the large-scale integration of wind and solar generation). Those collaborative efforts will require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, three additional opportunities for progress could offer special benefits for strengthening GSE preparedness. First, DOE and its industry partners should consider expanding the scope of EO planning across the energy sector to address the risk that adversaries will attack

both the grid and the natural gas transmission system on which power generation increasingly depends. Second, these partners should develop additional options to counter the risk that adversaries will conduct targeted information operations to sow disorder and magnify the disruptive effects of attacks on the grid. Third, government leaders should also explore strategic opportunities to capitalize on the improvements in grid resilience that EOs and related preparedness initiatives will make possible. In particular, these leaders should consider developing integrated offense-defense operational plans to strengthen the deterrence of cyberattacks against the United States, and to help manage the escalation (and speed the favorable resolution) of conflicts that do occur.

## **I. DEVELOPING EMERGENCY ORDERS UNDER THE FEDERAL POWER ACT: OVERARCHING GOALS AND DESIGN REQUIREMENTS**

The foundational importance of the electric grid makes it a prime target for attack. As Secretary of Energy Richard Perry emphasizes, “America’s greatness depends on a reliable, resilient electric grid” that can power the economy, support national defense, and provide for the necessities of modern life.<sup>2</sup> To prevent adversaries from exploiting this extraordinary dependence on the U.S. electric system, the Department of Energy and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter – and, if necessary, defeat – attacks on the grid.<sup>3</sup>

The text of the FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the “FAST Act” amendments to the FPA, legislators greatly expanded the Secretary of Energy’s authority to issue emergency orders to grid owners and operators. Under Section 215A of the Act, “the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgement of the Secretary to protect or restore the reliability” of the critical grid infrastructure in a grid security emergency.<sup>4</sup>

---

<sup>2</sup> Secretary of Energy Richard Perry, *Letter to the Federal Energy Regulatory Commission Re: Secretary of Energy’s Direction that the Federal Energy Regulatory Commission Issue Grid Resiliency Rules Pursuant to the Secretary’s Authority Under Section 403 of the Department of Energy Organization Act*, September 28, 2017, <https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf>.

<sup>3</sup> As noted above, the 2015 FAST Act amendments to the Federal Power Act (FPA) provide the authority to do so. Prior to 2015, Section 202(c) of the FPA already authorized the Secretary of Energy to issue emergency orders to order “temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest.” That provision also specified that the Secretary could exercise such powers “during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes.” See: “DOE’s Use of Federal Power Act Emergency Authority,” *Department of Energy*, 2017, <https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use>. The 2015 FAST Act amendments to the FPA gave the Secretary further powers (mostly incorporated in Section 215A of the Act), which are the primary focus of this study.

<sup>4</sup> Before the Secretary can issue emergency orders, the President must first declare a grid security emergency (GSE). The analysis that follows examines the definition of GSEs in the FPA. This analysis also examines the focus of

However, legislators provided only limited guidance on what the Secretary might order power companies to do. The Department of Energy and their partners in the electricity subsector have begun to assess which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats.

This portion of the study (Section I) examines the near and longer-term advantages of developing emergency orders before adversaries strike. Section I also identifies specific industry and government partners who might participate in this development process, and highlights the overall design requirements that emergency orders may need to meet, both to comply with the Federal Power Act and to address the broader challenges that grid security emergencies will pose.

The Act specifies that before the Secretary can issue emergency orders, the President must first declare a grid security emergency (GSE). Section II surveys the types of threats that can trigger a GSE and explains why this study focuses on the risk of cyber and physical attacks. Section II also examines possible thresholds and decision criteria that the President might use to determine whether a GSE exists, and how consultations and information sharing with power companies might support such determinations.

Section III provides a framework for developing emergency orders for use in three phases of GSEs: when the President determines that there is an imminent danger of attacks, when attacks are underway, and when electric companies are restoring power – potentially in the face of continuing attacks on the grid. Section III also provides examples of emergency orders (EOs) and identifies promising options for further analysis.

Section IV analyzes the broader design challenges that emergency orders may entail. These include: 1) tailoring EOs to help deter attacks on the United States, and help the U.S. military defeat adversaries if deterrence fails; 2) ensuring that the Secretary can effectively communicate emergency orders to power companies if phone and internet communications are disrupted, and pre-planning to communicate with the American people when attacks are underway; and 3) strengthening the “value added” of emergency orders for the electric industry by providing political top cover for unpopular emergency measures, as well as regulatory waivers and cost recovery beyond the provisions in the FPA. Section V identifies issues for further analysis that may offer special benefits for building preparedness for grid security emergencies.

## **A. IMPERATIVES FOR GOVERNMENT-INDUSTRY COLLABORATION**

The Secretary’s new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, “the nine most terrifying words in the English language are

---

emergency orders on protecting or restoring the reliability of critical electric infrastructure and defense critical electric infrastructure in the bulk power system (BPS), and the definition of these terms in the Act.



‘I’m from the government and I’m here to help.’”<sup>5</sup> Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already beginning to manage such risks by incorporating industry recommendations on the process by which the Secretary should issue emergency orders (EOs), and – “if practicable” – consult with industry before those orders are issued.<sup>6</sup> The next collaborative step should be to include power companies in designing EOs. Grid owners and operators have unequalled knowledge of their own infrastructure and operating procedures, and have extensive experience in employing emergency measures to protect and restore grid resilience. They are well-positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses – and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders will assist them in protecting or restoring grid reliability, above and beyond the emergency measures that companies would already be taking on their own.

Industry will need government leadership as well. Federal guidance will be essential to ensure that emergency orders help achieve overarching U.S. security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing EOs to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.<sup>7</sup> Federal leadership will also be necessary to integrate criteria and decisions for issuing emergency orders into the broader U.S. incident response system established by Presidential Policy Directive 41: *United States Cyber Incident Coordination* (July 2016), the *National Response Framework* (June 2016), and other mechanisms and guidelines for coordinating response operations.<sup>8</sup> In addition, as provided for in the FPA and other sources of Federal guidance, government agencies (with industry support) will also need to identify the grid infrastructure that is most critical for protecting the U.S. economy, public health and safety, and the defense of the United States.<sup>9</sup>

Government participation will also be necessary to account for the support that DOE and other agencies may be able provide to industry in grid security emergencies. For example, if adversaries destroy large power transformers and other critical grid infrastructure, Federal, state,

---

<sup>5</sup> Ronald Reagan, “The President’s News Conference,” August 12, 1986, <http://www.presidency.ucsb.edu/ws/?pid=37733>.

<sup>6</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1176; EEI, “COMMENTS OF THE EDISON ELECTRIC INSTITUTE,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*, February 6, 2017; and IRC, “ISO-RTO Council Comments on Notice of Proposed Rulemaking,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*, February 6, 2017.

<sup>7</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017.

<sup>8</sup> White House, *Presidential Policy Directive - United States Cyber Incident Coordination*, July 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>; Department of Homeland Security, *National Response Framework: Third Edition*, June 2016.

<sup>9</sup> 16 U.S.C. § 824o-1, Section (c), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

local, tribal, and territorial transportation agencies may be able to waive regulations and other requirements that would otherwise slow the movement of replacement transformers. The Department of Energy may not be able to order transportation agencies to issue such waivers. However, DOE can lead government-wide engagement to incorporate waiver planning and other support functions into emergency orders and provide a focal point for industry collaboration.<sup>10</sup> Most important of all: DOE is the Sector-Specific Agency for the energy sector and is uniquely positioned to partner with electric utilities in the EO development process.

## **1. Drafting Template Emergency Orders Before Attacks Occur**

The Federal Power Act specifies that before issuing emergency orders “the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action,” consult with appropriate power companies and other stakeholders in grid resilience.<sup>11</sup> In January 2018, the Department of Energy issued procedures for conducting such consultations and communicating emergency orders, and incorporated a number of recommendations proposed by power companies to strengthen industry-government coordination in grid security emergencies.<sup>12</sup>

But the need for action may be too urgent to permit such consultation before the Secretary issues emergency orders. Adversaries may launch cyberattacks on the grid with little or no warning. Indeed, they will have additional incentives to do so if they can preclude the effective use of emergency orders by minimizing opportunities for industry-government dialogue, and by disrupting communications between DOE and grid owners and operators.

To ensure that EOs will benefit from industry-government consultation, and to minimize the risk that DOE will have to design orders from scratch amidst the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, Assistant Secretary of Energy for Electricity Delivery and Energy Reliability, stated in March 2018 that “In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.”<sup>13</sup> Power companies and other

---

<sup>10</sup> The FAST Act amendments explicitly provide for such a role in cybersecurity planning and incident management. See: “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1779, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>11</sup> 16 U.S. Code § 824o-1, <https://www.law.cornell.edu/uscode/text/16/824o-1>. See also the notice of proposed rulemaking and request for comment: Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 81, No. 235 (2016), [https://energy.gov/sites/prod/files/2017/02/f34/DOE\\_FRDOC\\_0001-3281.pdf](https://energy.gov/sites/prod/files/2017/02/f34/DOE_FRDOC_0001-3281.pdf).

<sup>12</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1175.

<sup>13</sup> Bruce J. Walker, *Written Testimony Before the U.S. Senate Committee on Energy and Natural Resources*, March 1, 2018, [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=1C574731-A9C0-4E1C-9E05-15C492E332B1](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1)

electricity subsector organizations have also emphasized the need for industry and government to jointly develop orders before adversaries strike.<sup>14</sup>

Such collaborative efforts should initially focus on creating *template orders*: i.e., orders that lay out the basic types of actions that the Secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act’s potential value for the Secretary to issue general orders to “protect and restore the reliability of the grid.” Vague, overly broad directives cannot provide an adequate basis for utilities to build system-specific plans to implement them, or exercise and train utility personnel to do so. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for “maximum generation” and increased reserve margins to more aggressive, far-reaching measures.<sup>15</sup> The goals for such development efforts: 1) provide a menu of pre-agreed upon options from which the Secretary can choose as circumstances require, in consultation with industry (as provided for in the FPA); and 2) ensure that existing utility plans for prioritized power restoration and other emergency operations help achieve government-identified national security priorities.

In actual attacks, Russia, China, or other potential adversaries will employ country-specific malware and tactics, techniques, and procedures. Defense against those attacks will require equally tailored, threat-specific tactical and operational response measures. Over time, it may be possible to develop (and protect adversaries from stealing) emergency orders that account for these individualized defensive requirements. U.S. leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this study will examine the development of such integrated offense-defense plans as a future research priority.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military

---

<sup>14</sup> See: Joint Commenters, “COMMENTS OF AMERICAN PUBLIC POWER ASSOCIATION, LARGE PUBLIC POWER COUNCIL, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, AND TRANSMISSION ACCESS POLICY STUDY GROUP,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, February 23, 2017, <http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf>; NASEO, “COMMENTS OF THE NATIONAL ASSOCIATION OF STATE ENERGY OFFICIALS,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, n.d.a, [https://www.naseo.org/Data/Sites/1/naseo-comments\\_rin-1901-ab40.pdf](https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901-ab40.pdf); and EEI, “COMMENTS OF THE EDISON ELECTRIC INSTITUTE,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, February 6, 2017.

<sup>15</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help “maintain reliable operation while meeting ... unexpected outages of existing capacity.” See: NERC, “M-1 Reserve Margin,” 2017, <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.

bases, regional hospitals, and other critical facilities in their service area that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and present opportunities to improve order design and coordination. Training programs to prepare employees to carry out utility-specific plans to implement template orders should also get underway as soon as those orders are developed. On a larger scale, utilities will also be able to plan and exercise for the employment of template emergency orders under the Cyber Mutual Assistance (CMA) program. This program enables over a hundred utilities to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.<sup>16</sup> As the CMA program grows, it will provide increasingly valuable support for the nationwide execution of emergency orders.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the Secretary of Energy has the sole authority to issue EOs, the Secretary may request input from senior DOE staff on the benefits of specific options and the rationale for issuing those orders. The Secretary and DOE staffers may also need to brief the President and the National Security Council on proposed orders and the public messaging issues the orders entail. By developing EOs before GSEs occur and explaining how they will protect grid reliability, DOE and industry partners can strengthen the foundations for such deliberations and help design exercises for GSE decision making.

Over the longer term, industry and government leaders might structure their collaboration in order to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public-private and interagency coordination.<sup>17</sup> Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government-industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, the development of template emergency orders and contingency plans to implement them will require power companies to conduct extensive operational and engineering studies. The FAST Act amendments to the FPA provide no funding for such development efforts.

---

<sup>16</sup> “The ESCC’s Cyber Mutual Assistance Program,” *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1>.

<sup>17</sup> Richard Danzig, “Catastrophic Bioterrorism – What Is To Be Done?,” *Center for Technology and National Security Policy*, August 2003, [http://www.response-analytics.org/images/Danzig\\_Bioterror\\_Paper.pdf](http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf), pp. 5-7; Blue Ribbon Study Panel on Biodefense (Hudson Institute), *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts – Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*, October 2015, <http://www.biodefensestudy.org/a-national-blueprint-for-biodefense>, pp. 13 and 42-4.

Moreover, in order to build and effectively execute such plans, power companies will need to coordinate (and potentially share sensitive information) with a much wider array of partners as the development process goes forward.

## **2. The Bulk Power System as the Focus of GSE Declarations and Emergency Orders: Implications for EO Development**

Before examining these design requirements in further detail, an underlying constraint in the Federal Power Act merits analysis. The Act specifies that critical electric infrastructure includes only those assets that comprise the bulk power system (BPS). BPS assets are those “facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation facilities needed to maintain transmission system reliability.”<sup>18</sup> These bulk power system generation and transmission assets provide synchronized power across the three interconnections that serve the entire United States and parts of Mexico and Canada.<sup>19</sup>

However, as defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.<sup>20</sup> The FPA also specifies that emergency orders will apply to BPS owners and operators. That focus excludes local distribution providers, even if they provide the “last mile” of connectivity between transmission systems and military bases and other critical customers. The exclusion of local distribution providers has significant implications for the design and implementation of EOs, and poses political as well as technical challenges for protecting and restoring electric service.

The FPA states that the Secretary of Energy may issue emergency orders to a range of BPS “entities.”<sup>21</sup> These include:

***a. The Electric Reliability Organization.*** After blackouts cascaded across major portions of the United States in August 2003, Congress directed the Federal Energy Reliability Commission (FERC) to designate an Electric Reliability Organization (ERO) to enforce mandatory electric reliability rules on all users, owners, and operators of the U.S. bulk power system.<sup>22</sup> FERC appointed the North American Electric Reliability Corporation (NERC) as the first ever ERO in July 2006, and it has served in that role since.<sup>23</sup> NERC’s mission is to assure the reliability and

---

<sup>18</sup> 16 U.S.C. § 824o, Section (a)(1), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>19</sup> Interconnections are defined as the “geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control.” North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See: “Glossary of Terms Used in NERC Reliability Standards,” *NERC*, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

<sup>20</sup> The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify “local” distribution. See: 16 U.S.C. § 824o, Section (a), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>21</sup> 16 U.S.C. § 824o–1, Section (b)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>22</sup> *Energy Policy Act*, Public Law 109-58, *U.S. Statutes at Large* 119 (2005): pp. 942-943.

<sup>23</sup> NERC, *History of NERC*, August 2013, <http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf>.

For more information on NERC, see: “About NERC,” *NERC*, n.d.a, <http://www.nerc.com/AboutNERC/Pages/default.aspx>.



security of the BPS in North America. As such, NERC will be a key partner in developing template emergency orders, especially to help defeat attacks that could create cascading blackouts or other multi-state disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a critical role for the electric subsector in establishing situational awareness, incident management and coordination, and communication capabilities.<sup>24</sup> E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be particularly vital in consultations on issuing and refining emergency orders against specific threats.

***b. Regional entities responsible for enforcing reliability standards for the bulk power system.***<sup>25</sup> NERC delegates its authority to monitor and enforce compliance with reliability standards to eight regional entities which “account for virtually all the electricity supplied in the United States.”<sup>26</sup> While regional entities play crucial oversight roles, they do not directly operate the grid and would not, on their own, be positioned to execute emergency orders to protect or restore reliability. They will nonetheless play an important role regarding waivers for legal and regulatory compliance, as will be examined in detail in Section IV.

***c. Owners, users and operators of critical electric infrastructure (CEI) or defense critical electric infrastructure (DCEI) within the United States.***<sup>27</sup> When the President declares a grid security emergency, issuing emergency orders to power companies that own and operate generation and transmission assets will offer crucial opportunities to protect grid reliability. In addition, Reliability Coordinators (RCs) will play essential roles in designing and implementing emergency orders. RCs are the entities that constitute “the highest level of authority” for the reliable operation of the bulk electric system.<sup>28</sup> RCs are also responsible for maintaining a “wide

---

<sup>24</sup> “Electricity ISAC,” NERC, n.d.a, <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>25</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177. See also: 16 U.S.C. § 824o, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>26</sup> “Key Players,” *North American Electric Reliability Corporation*, n.d.a., <https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>. One regional entity, however, announced its intention to dissolve in July 2017, currently pending final FERC approval. See: North American Electric Reliability Corporation, “JOINT PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION, MIDWEST RELIABILITY ORGANIZATION, AND SERC RELIABILITY CORPORATION FOR APPROVALS IN CONNECTION WITH THE DISSOLUTION OF THE SOUTHWEST POWER POOL REGIONAL ENTITY,” *Filing Before the Federal Energy Regulatory Commission* (Docket No. RR18-3-000), <https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/SPP%20Dissolution%20Petition.pdf>.

<sup>27</sup> The analysis that follows later in this section examines the definition of “users” of critical electric infrastructure, as well as defense critical electric infrastructure.

<sup>28</sup> While the Bulk Power System (BPS) broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the Bulk Electric System (BES) is a subset of the BPS which includes, with some exclusions, all transmission and real and reactive power sources at 100 kV or higher. As with the BPS, the BES definition excludes local distribution providers. For these definitions, as well as the definition of Reliability Coordinators, see: “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf). Consistent with the FPA and the authorities it provides for

area view” of the bulk electric system, and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, RCs will be critical for designing, receiving, and implementing emergency orders to counter attacks that may exceed the ability of individual BPS system owners and operators to defeat. Seven Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) also help operate and ensure the reliability of the bulk electric system in many regions of the United States.<sup>29</sup> Accordingly, RTOs and ISOs will be essential to the design and execution of emergency orders.

#### ***d. Local Distribution Providers***

The role of distribution systems in responding to grid security emergencies is less clear-cut. As noted above, the Federal Power Act only authorizes the Secretary to issue emergency orders to bulk power system entities. The Act does not explicitly authorize the Secretary to issue emergency orders to utilities that provide for local distribution of electric power. Nevertheless, local distribution infrastructure may play a vital role in protecting the flow of power to key facilities in grid security emergencies. Even if emergency orders can help defeat attacks on the bulk power system, adversaries may still be able to achieve catastrophic effects by attacking multiple local distribution systems, and thereby interrupt the flow of power from transmission systems to hospitals and other end users. A holistic approach to GSE preparedness will need to account for these risks to local infrastructure.

Integrating local distribution systems into planning for grid security emergencies will also be useful from an operational perspective. Even though local distribution utilities may not themselves be subject to EOs, they may be functionally required to help implement such orders. For example, if the Secretary orders transmission systems to shed load to protect grid reliability, while also preserving the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding.

From an historical perspective, it is understandable why the FPA does not explicitly account for local distribution utilities in grid security emergency operations. State public utility commissions have long had regulatory jurisdiction over distribution systems. Any legislative effort to give the Secretary of Energy emergency authorities over local distribution assets could have created strong opposition from state leaders and their defenders in Congress.<sup>30</sup> Nevertheless, if the

---

handling grid security emergencies, this study focuses on the application of emergency orders to BPS entities specifically.

<sup>29</sup> There are 10 RTOs and ISOs under NERC’s purview, though three operate exclusively in Canada. RTOs and ISOs are independent, membership-based, non-profit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are operated by individual utilities or utility holding companies. “About 60% of the U.S. electric power supply is managed by RTOs,” *U.S. Energy Information Administration*, April 4, 2011, <https://www.eia.gov/todayinenergy/detail.php?id=790>. Six of the seven RTOs/ISOs are also current reliability coordinators. See: “Reliability Coordinators,” *North American Electric Reliability Corporation*, n.d.a., <https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.

<sup>30</sup> The U.S. Constitution, in most cases, only allows Federal regulation of private economic activity for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See: Jim Lazar (for The Regulatory Assistance Project), *Electricity Regulation in the US: A Guide*, 2<sup>nd</sup> Edition, June 2016, p. 15.

United States is to prevent grid-wide attacks from jeopardizing national security, economic security, or public health or safety, extensive coordination and collaboration with local distribution systems will be essential.

An initial step toward building such an integrated approach will be to specify which distribution facilities that serve CEI and DCEI are “local.” As FERC notes, the FPA’s BPS definition “does not establish a voltage threshold limit of applicability or configuration.” The definition instead relies on the functional requirement of “necessary for operating an interconnected electric energy transmission network” set out by the FPA.<sup>31</sup>

Local distribution utilities which are not necessary for such interconnected operations may nevertheless provide the “last mile” of power delivery to military bases and other vital facilities. It might be possible to interpret the FPA as making emergency order applicable to these utilities as well. The Act states that emergency orders may apply to “any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure” within the United States. The Act, however, does not further define owners, users and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the Act.

Even if the Secretary cannot issue orders directly to such utilities, BPS entities should still include them in building the contingency plans necessary to implement emergency orders. Before BPS owners and operators receive EOs, they could pre-plan to coordinate with local distribution systems to strengthen comprehensive, end-to-end protection of grid reliability for critical customers. Many companies that own transmission assets also own distribution infrastructure, simplifying coordination for EO planning purposes. Integrated planning will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for “vertically integrated” utilities that own and operate assets for all three functions.

However, while many investor-owned utilities are vertically integrated, municipally-owned electric utilities and rural electric cooperatives (which serve a significant amount of CEI and DCEI) are not. In the many regions of the United States where generation, transmission, and distribution systems exist as separate, non-integrated companies, additional engagement

---

<sup>31</sup> Federal Energy Regulatory Commission, *Revision to Electric Reliability Organization Definition of Bulk Electric System* (Order No. 743), 133 FERC ¶ 61,150, November 18, 2010, pp. 22-24. FERC and NERC have also defined the Bulk Electric System (BES), a subset of the BPS, for regulatory purposes. Unlike the FPA’s BPS definition, NERC’s core BES definition establishes a uniform “bright line” threshold of 100 kV. Accordingly, the BES includes “all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher,” with specific, additional criteria for inclusions and exclusions to provide further clarity. NERC also established an exception process through their Rules of Procedure to make additional inclusions and exclusions on a case-by-case basis. FERC accepted the definition in 2012 (Docket Nos. RM12-6-000 and RM12-7-000; Order No. 773), and the FERC decision was upheld by the Second Circuit Court of Appeals, in *New York V. FERC*, 783 F.3d 946 (2d Cir. 2015). See: Federal Energy Regulatory Commission, *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure* (Order No. 773-A), 143 FERC ¶ 61,053, April 18, 2013, pp. 2-7; and “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

measures will be essential to help effectively implement EOs. As the Federal government identifies critical facilities for prioritized protection and restoration of power, BPS entities that provide the electricity on which those facilities rely should ensure that local distribution systems are included in designing and implementing orders for prioritized emergency service.

#### *e. Additional Partners for Engagement*

As the Department of Energy and the electricity subsector develop emergency orders, they should identify and pre-plan with other partners who can assist in executing those orders. The GSE Rule notes that “Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits” to expedite the restoration of power.<sup>32</sup> Still broader collaboration with government and private sector partners may be valuable for implementing EOs to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy Large Power Transformers (LPTs) at substations across the United States, and these attacks cut off power to critical military bases, the Secretary might order industry to prioritize the replacement of LPTs at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program (STEP) to provide for such replacements,<sup>33</sup> and new industry-led organizations such as Grid Assurance and the Regional Equipment Sharing for Transmission Outage Restoration Agreement (RESTORE – a mutual assistance-like agreement for enabling transfers of transformers and other critical equipment recently approved by FERC).<sup>34</sup> These initiatives further strengthen the industry’s LPT resilience posture in ways that could be valuable for restoration operations in grid security emergencies.

However, power companies do not move LPTs by themselves. They rely on railroad companies, barges, and “heavy hauler” trucking companies to help do so, and have established a Transformer Transportation Working Group (TTWG) to plan and coordinate LPT movement operations.<sup>35</sup> The FPA does not give the Secretary authority to issue orders to transportation companies. Nevertheless, in anticipation of orders for transformer movement, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Pre-coordinating with the U.S. Department of Transportation and state governments to get permits and regulatory waivers to expedite transformer movement will also be helpful.

---

<sup>32</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177.

<sup>33</sup> See: Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>; and “Spare Transformers,” *Edison Electric Institute*, n.d.a, <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.

<sup>34</sup> Federal Energy Regulatory Commission, *ORDER AUTHORIZING ACQUISITION AND DISPOSITION OF JURISDICTIONAL FACILITIES* (163 FERC ¶ 61,005), April 3, 2018, p. 10, <https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf>.

<sup>35</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 12, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

Equally valuable partnership opportunities will emerge in designing and pre-planning for the execution of other emergency orders. For example, when the Secretary issues an emergency order, agencies and utilities should already have determined what they will tell the public about the purpose of the order, its expected impact on electric service, and -- ideally -- when normal service will be restored. Identifying these and other partnership requirements will be critical as the design process goes forward.

### **3. Template Emergency Orders: Goals and Specific Design Requirements**

The starting point to develop template emergency orders is to identify the objectives and design requirements that these orders will need to encompass, and clarify the underlying policy challenges that the EO development process will need to address. Key issues analyzed in the next sections of the study:

- Threats, Triggers and Thresholds for Issuing Emergency Orders. The Federal Power Act requires the President to have declared a “grid security emergency” (GSE) before the Secretary can issue emergency orders.<sup>36</sup> Only a limited number of natural and manmade hazards can trigger a GSE. Countering each of those hazards will require different, threat-specific specific emergency orders. Hence, the first step for developing such orders will be to select the threats on which the design process should focus.

The Act authorizes the President to declare a GSE when there is an “imminent danger” of attacks on critical grid infrastructure, or when attacks are occurring.<sup>37</sup> Different types of emergency orders will be needed to preserve grid reliability 1) when attacks are imminent, and 2) when attacks are underway. Promising opportunities also exist to develop orders for a third phase of GSE operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.

- Incorporating National Security Policies and Priorities into GSE Order Design. The FPA’s definition of grid security emergencies helps frame the order design process in an additional way. GSEs exist when adversaries pose serious threats to:
  - *Critical electric infrastructure*, which is comprised of grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters;”<sup>38</sup> and
  - *Defense critical electric infrastructure*, which serves facilities that are “critical to the defense of the United States” and are vulnerable to the disruption of grid-provided power.<sup>39</sup>

---

<sup>36</sup> Along with cyberattacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>37</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>38</sup> 16 U.S.C. § 824o–1, Section (a)(2), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>39</sup> 16 U.S.C. § 824o–1, Section (a)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.



Government and industry partners should design emergency orders to protect and restore the reliability of these high-priority grid systems and the customers they serve.

Emergency orders should also reflect broader Federal government strategies to defend critical infrastructure. The U.S. *National Security Strategy*, for example, provides crucial guidance on how the United States will deter attacks on critical systems, and -- if deterrence fails -- defeat the attackers.<sup>40</sup> DOE and its industry partners should design emergency orders to help implement the Strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this strategic design process with two further steps. First, building on the provisions of the FPA and on existing industry plans to prioritize the restoration of power, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement EOs and help defend the nation.

- Communications. The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The Rule on Procedures for Issuance of emergency orders (hereinafter referred to as the ‘GSE Rule’) provides a description of the consultative process that (if practicable) will occur before the Secretary sends such orders.<sup>41</sup> However, the GSE Rule does not address the risk that adversaries will attack the industry-government communications systems necessary to issue orders, monitor their compliance, and defeat adversary attacks. Building secure, survivable communications will be essential to the effective use of emergency orders to protect or restore grid reliability. However, the FPA establishes no requirements or funding to do so. Industry and government partners should consider including secure communications as a crucial component of the overall GSE preparedness effort, lest those potential vulnerabilities be left for adversaries to exploit.

Government and utility leaders will also need to coordinate what they tell the American people when the Secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including EOs for prioritized load shedding, could cut off electricity to many thousands of customers in order to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by pre-planned communications playbooks to address customer concerns.

Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Adversaries will strike the grid to achieve

---

<sup>40</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 13.

<sup>41</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1181.

political benefits, including, potentially, the incitement of public panic and a loss of confidence in U.S. leaders. Building upon existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders, will be essential to provide for unity of messaging against such efforts.

- Waivers and Cost Recovery. Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the Act, FERC-approved reliability standards, or environmental regulations.<sup>42</sup> However, potentially valuable emergency orders will be easier to implement if they include pre-planned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.<sup>43</sup> Industry-government dialog will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader pre-planning needed for the financial challenges that grid security emergencies could create, including the catastrophic loss of power company revenue and the breakdown of company access to emergency loans or other financial instruments.

## **II. THREATS, TRIGGERS, AND CONSULTATIVE OPTIONS FOR DECLARING GRID SECURITY EMERGENCIES**

The Federal Power Act leaves the President substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should also consider seeking consensus on the types of threats that on which the development process should focus, and establish decision criteria and consultative mechanisms to support GSE declarations.

### **A. THREATS THAT CAN TRIGGER GRID SECURITY EMERGENCIES: IMPLICATIONS FOR EO DESIGN**

A broad array of natural and manmade hazards can cause multi-state blackouts, including earthquakes and severe weather events such as hurricanes and ice storms. However, in amending the Federal Power Act, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the “occurrence or imminent danger” of:

- 1) “A malicious act using **electronic communication** or an **electromagnetic pulse**, or a **geomagnetic storm** event, that could disrupt the operation of those electronic devices or

---

<sup>42</sup> These waivers apply unless companies carry out orders and related actions in a “grossly negligent manner.” See: 16 U.S.C. § 824o-1, Section (f)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>43</sup> 16 U.S.C. § 824o-1, Section (b)(6), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;”<sup>44</sup> and

2) “Disruption of the operation of such devices or networks, with significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event;” or

3) “A **direct physical attack** on critical electric infrastructure or on defense critical electric infrastructure;” and

4) “Significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.”<sup>45</sup>

Protecting CEI and DCEI against each of these threats will require different types of emergency orders. The threats will also pose disparate challenges for determining the imminence or occurrence of a grid security emergency, ranging from relatively simple to deeply problematic. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the President faces uncertainties about the likelihood and potential consequences of a GSE.

### **1. Geomagnetic Storms as a Possible Initial Focus**

Emergency orders against geomagnetic disturbances (GMD) will entail fewer design challenges than for cyberattacks and other manmade hazards, and could therefore provide opportunities for relatively rapid progress in strengthening GSE preparedness. GMD events occur when coronal mass ejections on the sun create geomagnetically induced currents (GICs) on the surface of the earth. These currents can damage unprotected transformers and other grid infrastructure. Compared to the other threats that can trigger grid security emergencies, determining that there is an imminent danger of a GMD event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the President decide whether to declare a GSE, and will provide hours of warning before the solar energy begins creating destructive GICs.

Industry and government partners can develop emergency orders that exploit this warning time. For example, the Secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of ground induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.<sup>46</sup>

---

<sup>44</sup> Section II of this paper defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of GSE thresholds.

<sup>45</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>46</sup> Dr. Tony Phillips, “Solar Shield--Protecting the North American Power Grid,” NASA, October 26, 2010, [https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\\_solarshield](https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield). See also: MISO, *Geomagnetic Disturbance Operations Plan* (SO-P-AOP-01 Rev: 1), June 9, 2017, p. 5, <https://www.misoenergy.org/Library/Repository/Procedure/SO-P-AOP-01%20Geomagnetic%20Disturbance%20Operations%20Plan.pdf>.

A strong foundation already exists for drafting such orders. Studies of GMD effects on the power grid have generated a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.<sup>47</sup> Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the Federal Government to ensure that it has the capability to predict and detect space weather events, the ability to communicate these assessments to public and private sector stakeholders, protection and mitigation plans for critical infrastructure, and response and recovery plans for GMD events. The order requires Sector-Specific Agencies to “assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event.”<sup>48</sup> NERC standards also exist for addressing GMD threats. TPL-007-1 – *Transmission System Planned Performance for Geomagnetic Disturbance Events* establishes long-lead GMD planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat (DBT) for GMD events.<sup>49</sup> EOP-010-1 – *Geomagnetic Disturbance Operations* also requires Reliability Coordinators to develop GMD mitigation plans and operating procedures, including specific actions that Transmission Operators must take based on predetermined GMD-related conditions.<sup>50</sup>

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyberattacks and other manmade triggers for grid security emergencies. The sun will not intentionally hide preparations for a GMD event or “prepare the battlefield” by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data utility personnel need to maintain situation awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of CEI and DCEI.

The relative ease of drafting orders for geomagnetic disturbances makes such GMD efforts a prime starting point for industry-government collaboration. The North American Transmission Forum (NATF), in coordination with the ESCC, is already examining opportunities to develop template emergency orders for GMD events. But the greater degree of difficulty associated with

---

<sup>47</sup> See: National Oceanic and Atmospheric Administration, *NOAA Space Weather Scales*, April 2011, <https://www.swpc.noaa.gov/sites/default/files/images/NOAAscales.pdf>; Metatech (for Oak Ridge National Laboratory), *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*, January 2010, [https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc\\_meta-r-319.pdf](https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf).

<sup>48</sup> The White House, *Executive Order -- Coordinating Efforts to Prepare the Nation for Space Weather Events*, October 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events>.

<sup>49</sup> NERC, *TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events*, December 2014, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States).

<sup>50</sup> The standard, however, does not explicitly lay out what those predetermined conditions should be. See: NERC, *EOP-010-1 – Geomagnetic Disturbance Operations*, June 2014, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States). For an example of GMD plans, see: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, pp. 69-71.

protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of EOs to counter such threats. Instead, DOE and its industry partners should consider pursuing a multi-track development process: at the same time that they seek rapid progress on emergency orders for GMD, they should *immediately* accelerate the long-lead work that will be required against each of the manmade threats that can trigger grid security emergencies.

## **2. Cyber and Physical Attacks**

This study focuses on supporting the development of EOs to protect and restore grid reliability against cyberattacks. The U.S. *National Security Strategy* highlights the imperative to counter the intensifying cyber threats to the grid and other critical infrastructure. The Strategy warns that the vulnerability of U.S. critical infrastructure to cyberattacks and other threats “means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and communications.” Cyber weapons also “enable adversaries to attempt strategic attacks against the United States – without resorting to nuclear weapons – in ways that could cripple our economy and our ability to deploy our military forces.”<sup>51</sup> An immediate focus for EO development efforts should be to help counter such potentially devastating cyber threats, by designing orders to protect or rapidly restore electric service to military bases and civilian-owned facilities vital to the economy and public health and safety.

This study also examines the development of emergency orders against physical attacks on the grid. Since the carefully coordinated attack against the Metcalf, California substation in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high powered rifles or other weapons.<sup>52</sup> Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

Launching physical attacks would entail risks to the adversary beyond those created by cyberattacks. Blowing up transformers and -- potentially -- killing workers who are transporting replacement equipment would immediately escalate conflict with the United States into open kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries will hide on utility networks, arming and pre-positioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

---

<sup>51</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, pp. 12 and 27, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

<sup>52</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation’s Electricity System: Second Installment of the QER*, January 2017, p. 4-34; NERC, *CIP-014-02: Physical Security*, effective October 2, 2015, <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.



Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk-reward calculus in our favor. If EOs can help power companies protect their systems from physical attacks, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Grid owners and operators are also strengthening their preparedness against combined cyber-physical attacks. Such combined attacks can create synergistic disruptions of the grid beyond those from cyber or physical attacks on their own. For example, as in the response to the cyberattacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.<sup>53</sup> Attacks that physically destroy critical components at those substations or shoot utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

To prepare against such difficult challenges, the largest-scale exercise conducted by NERC and the electricity subsector, GridEx, uses combined cyber-kinetic attacks on power companies in multiple U.S. regions as the exercise's scenario. GridEx also assumes that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging far more difficult than in any past U.S. power outage.

This study adopts a similarly severe threat for analyzing possible EOs. In particular, the study examines how orders can protect or restore grid reliability against the combined use of cyber weapons, kinetic strikes, and information warfare against critical electric infrastructure and defense critical electric infrastructure. Of course, separate types of emergency orders will be required against physical and cyberattacks. Orders to deploy additional armed guards to substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead and accounting for the risk of combined attacks will provide valuable context for the development of physical and cyber EOs, and for the public communications support they will require.

The study does not examine options for developing emergency orders against electromagnetic pulse attacks. EMP threats pose a significant potential risk to the grid, and a growing number of utilities are hardening their critical systems against EMP effects.<sup>54</sup> The Department of Energy's EMP strategy provides a valuable framework approach for managing the risks that EMP threats

---

<sup>53</sup> E-ISAC and SANS-ICS, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, March 2016, p. v.

<sup>54</sup> In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to GMDs. The early-time (E1) component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See: Electric Power Research Institute, *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research* (3002000796), December 2013, pp. 3-3-3-4.

pose to the grid and other energy systems.<sup>55</sup> The Department of Homeland Security’s EMP strategy does the same for a broad range of infrastructure sectors.<sup>56</sup> However, significant research will still be required to understand the combined effects of EMP wave components on grid hardware and system-wide operations, and on cost-effective mitigation options and preparedness planning.<sup>57</sup> As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

## **B. THRESHOLDS FOR DECLARING GRID SECURITY EMERGENCIES**

The President can declare a grid security emergency when there is either imminent danger of an attack or when attacks are already occurring.<sup>58</sup> These two circumstances for declaring a GSE will require distinct, sequential types of emergency orders: 1) pre-attack orders to “raise the gates” against imminent cyber and/or physical strikes; and 2) orders to protect grid reliability once attacks are underway, including measures to prevent the spread of cascading failures across critical and defense critical electric infrastructure. DOE and its partners should also consider developing specialized EOs for a third phase of grid security emergencies: operations to accelerate the restoration of power after adversaries have inflicted major blackouts.

Before attacks occur, pre-emptive orders could help grid owners and operators initiate *conservative operations* to reduce the vulnerability of their systems to attack, increase power reserves, and take other measures to manage the grid instabilities that adversaries may seek to create. Power companies already have extensive experience in employing conservative operations (COs) when hurricanes or other severe weather events are approaching. This experience provides a strong foundation on which to develop COs against cyber and physical attacks. However, determining that attacks are imminent can be vastly more difficult than assessing whether a hurricane will strike, especially if adversaries seek to achieve surprise.

A strong foundation also exists to build emergency orders for attacks that are underway. Most important, BPS entities already have plans and capabilities in place to protect grid reliability when major disturbances occur, and reduce the risk that such disturbances will create cascading failures or other widespread disruptions of electric service.<sup>59</sup> For example, NERC already

---

<sup>55</sup> The Department of Energy has set strategic goals for addressing EMP threats, and created an action plan to meet those goals. Department of Energy, *Electromagnetic Pulse Resilience Action Plan*, January 2017; The FY17 NDAA directed DHS to create a similar strategy, which is currently in draft form. “National Defense Authorization Act for Fiscal Year 2017,” Public Law 114-328, *U.S. Statutes at Large* 130 (2016): pp. 2685-2687; and the Electric Power Research Institute (EPRI) continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs* (3002008999), September 2016.

<sup>56</sup> Department of Homeland Security, *Strategy for Protecting and Preparing the Homeland Against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*, forthcoming (Spring 2018).

<sup>57</sup> Idaho National Laboratory, *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*, January 2016.

<sup>58</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>59</sup> The section that follows examines how NERC’s definition of “Adequate level of Reliability” for the Bulk Power System, including the prevention of cascading failures, can be used to help build design standards for emergency order and thresholds for declaring grid security emergencies. North American Electric Reliability Corporation,

requires transmission operators to be able to shed load (i.e., temporarily curtail or cut off electric service to customers) to mitigate operational emergencies.<sup>60</sup> Emergency orders should be developed for equivalent *extraordinary measures* to protect grid reliability.

A third category of emergency orders will also be valuable if (despite such extraordinary measures) attackers are able to create blackouts that jeopardize public health and safety, the U.S. economy, or national security. Electric industry stakeholders should design EOs to *accelerate restoration* of power to critical electric infrastructure and defense critical electric infrastructure if these blackouts occur. The Secretary could also issue such orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these customers. But lists that identify other national security-related assets, including components of the Defense Industrial Base and transportation infrastructure essential for deploying and sustaining military forces abroad, may be closely held by DOD and not yet included in industry restoration priorities. This study will examine how DOE and its industry partners can leverage existing government schemes for identifying critical facilities to help develop and execute EOs for restoration support, and how that sensitive data can be shared with power companies while remaining protected from adversaries.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, EOs for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are underway. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies “stop the bleeding” from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are underway.<sup>61</sup>

DOE and its partners will need considerable flexibility to deal with overlapping GSE phases in designing, issuing, and implementing executive orders. Nevertheless, being able to “rack and stack” potential orders in terms of when they would be issued and which phases of emergency operations they would support can help facilitate a structured, integrated approach to EO development.

---

“Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013.

<sup>60</sup> North American Electric Reliability Corporation, *EOP-011-1: Emergency Operations*, effective April 1, 2017, R1.2.5, [https://www.nerc.com/\\_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).

<sup>61</sup> In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is full restored to pre-event conditions) as the “New Normal” – characterized by “degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months.” See: North American Electric Reliability Corporation, *Severe Impact Resilience: Considerations and Recommendations*, May 9, 2012, pp. 14 and 16.

## **1. Determining When Attacks are Imminent: Criteria for Declaring GSEs and Issuing Emergency Orders**

The Federal Power Act defines GSEs as occurring when attacks that are imminent or underway “could disrupt the operation” of devices or networks that are “essential to the reliability of critical electric infrastructure or defense critical electric infrastructure.”<sup>62</sup> But the Act does not define imminent. Nor does it clarify the degree of potential disruption that will trigger the declaration of a GSE or detail the criteria that the President should use to make such a decision.

In key respects, the BPS system is under cyberattack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant APTs on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS systems, secrete malware designed to disrupt grid operations, and conduct other malicious activity to prepare for possible attacks on critical system components.<sup>63</sup> PJM Interconnection’s former CEO, Terry Boston, said the RTO experiences 3,000-4,000 hacking attempts *every month*.<sup>64</sup> Penetration efforts on a similarly massive scale are likely to be occurring against BPS entities across the United States. And, as in the case of Black Energy and other adversary campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.<sup>65</sup>

The President could conceivably decide that such campaigns constitute “occurring” attacks under the FPA that should trigger the declaration of a grid security emergency (and, presumably, the use of appropriate countermeasures against the perpetrator). Alternatively, the President might take these measures as evidence that there is “imminent danger” of an attack, and declare a GSE before adversaries used embedded malware to disrupt the operation of devices or networks essential to the reliability of CEI or DCEI.

Federal decision makers could also decide to set the threshold much higher. For example, the President might only declare a grid security emergency if adversaries were poised to disrupt CEI and DCEI across multiple regions of the United States, and could sustain those disruptions for a week or more. The text of the Federal Power Act leaves substantial ambiguity over the criteria that should trigger a GSE and justify the issuance of issue emergency orders to protect grid

---

<sup>62</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>63</sup> “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Readiness Team*, March 15, 2018, <https://www.us-cert.gov/ncas/alerts/TA18-074A>; “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Response Team (US-CERT)*, October 20, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-293A>; Defense Science Board, *Task Force on Cyber Deterrence*, February 2017, p. 4; ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*, June 2016, p. 19.

<sup>64</sup> Jon Dougherty, “Biggest U.S. power grid operator suffers thousands of attempted cyber attacks per month,” *Forward Observer*, August 22, 2017, <https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/>.

<sup>65</sup> Black Energy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of Black Energy inflicted the 2016 blackout on Ukraine. Alert (ICS-ALERT-14-281-01E), “*Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*, last updated December 9, 2016, <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.

reliability. In an intense crisis, this ambiguity could fuel disagreements amongst the President's advisors as to whether the threat of attack was sufficiently severe to declare a GSE, and unleash the firestorm of media speculation and congressional concern that a public declaration would produce.

But it would be a mistake to adopt a rigid set of GSE thresholds. Preserving broad latitude for the President to determine what constitutes a GSE will provide flexibility to deal with unforeseen circumstances and help avoid locking U.S. crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicly draw explicit "red lines" that would trigger a GSE. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay U.S. defensive measures, including the issuance of emergency orders to protect grid reliability. Adversaries might even seek to "spoof" the President into declaring a GSE when they had no intention of launching an attack – especially if doing so might incite public panic that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events which emergency orders should be designed to help counter. One option for clarifying such thresholds is to focus on the geographic scope of an emergency. In responding to DOE's *Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance*,<sup>66</sup> the ISO-RTO Council proposed that the use of emergency orders "should be reserved for true widespread emergencies." Equivalent criteria might be created by the President's advisors to support internal deliberations on whether to declare a GSE. However, additional options exist to assist such decision making in ways that are better attuned to the purposes of the Federal Power Act and offer more direct value for developing emergency orders.

## **2. Preventing Cascading Blackouts, Uncontrolled Separation, and other Disruptions of "Adequate Levels of Reliability"**

The North American Electric Reliability Corporation (NERC) has carefully defined what constitutes adequate reliability for the power grid, and the types of large-scale failures in reliability that owners and operators need to prevent. The imminent danger or occurrence of such failures should almost certainly be considered sufficient to declare a grid security emergency. The technical and operational requirements needed to prevent these failures also provide an opportunity to tailor emergency orders for each of them.

The 2003 Northeast blackout spurred efforts to define an adequate level of reliability for the grid and the system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over major portions of the United States, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The

---

<sup>66</sup> Theodore J. Paradise et al., "ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance—RIN 1901–AB40," *ISO-RTO Council*, February 6, 2017, [http://www.isorto.org/Documents/Report/20170206\\_Final\\_IRC-DOE\\_NOPR\\_Comments\\_re\\_Grid\\_Security\\_Emergency.pdf](http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf).



2005 amendments required FERC to certify an Electric Reliability Organization (ERO), which will have “the ability to develop and enforce ... reliability standards that provide for an adequate level of reliability of the bulk-power system.”<sup>67</sup> However, the EPA never defined “adequate level of reliability” (ALR); that task was left to the ERO to complete.

When NERC became the ERO in 2006, defining the ALR became one of its first initiatives. NERC’s Board of Trustees approved an initial definition for the “characteristics of a system with an adequate level of reliability” in 2008.<sup>68</sup> In May 2013, NERC released an updated ALR definition.<sup>69</sup> Three components of NERC’s definition are especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS, and to clarify the scale and scope of threats that EOs should be designed to counter.

The sections that follow examine each of these three components and the failures in reliability they can entail. However, in severe events, all three types of failures often occur in rapid succession and are inextricably linked. Protecting against their combined effects will be a key challenge in preparing for grid security emergencies.

**a. Instability.** NERC defines system instability as “the inability of the Transmission system to remain in synchronism ... characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES.”<sup>70</sup> The BES can experience frequency, voltage, or angular instability – though none should occur during normal operating conditions.<sup>71</sup>

Temporary instabilities occur occasionally; grid protection systems and operational protocols typically protect the bulk power system, mitigating their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, if BES generators accelerate or decelerate too much during a disturbance, the Transmission system may experience large power swings, causing transmission lines to trip and/or generators to go out of step and trip offline, resulting in further acceleration and deceleration.<sup>72</sup> Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread, cascading failures across CEI and DCEI. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur, given the speed at which instabilities propagate. Though difficult to predict, the determination that attackers were poised to both create instabilities and

---

<sup>67</sup> *Ibid.*

<sup>68</sup> North American Electric Reliability Corporation, *Technical Report Supporting Definition of Adequate Level of Reliability*, March 26, 2013, p. 17.

<sup>69</sup> The document refers to the Bulk Electric System (BES) rather than the Bulk Power System (BPS). See note 25 on differences between NERC’s BES and BPS definitions. Again, for the sake of clarity and consistency with the FPA this study uses the term BPS throughout.

<sup>70</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, p. 6.

<sup>71</sup> *Ibid.*, at pp. 1-2.

<sup>72</sup> *Ibid.*, at 6.

nullify protective systems could provide an additional basis for declaring a grid security emergency. Industry and government partners should explore the development of emergency orders for conservative operations to give the Transmission system extra “slack” to (ideally) avoid instabilities, as well as for extraordinary measures to help the system remain in synchronism should major instabilities occur.

**b. Cascading Failures.** NERC defines cascading as “the uncontrolled successive loss of system elements triggered by an incident at any location.” Such cascading “results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.”<sup>73</sup> NERC’s definition of the Adequate Level of Reliability (ALR) for the BPS states that the system will not experience cascading when struck by lightning strikes and other frequent, predictable incidents (i.e., “predefined Disturbances”). But more severe events have caused instabilities which led to cascading in the past and may do so again – especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout was especially wide-ranging and spurred the development of mandatory reliability standards to reduce the risk of such failures in the future. That blackout (which affected approximately 50 million people across the U.S. and Canada) started with a relatively minor incident. On a hot day in August, multiple 345-kV transmission lines tripped after sagging into overgrown trees. While operator actions might have been able to handle such a contingency with proper situational awareness, failures in the utility’s control room alarm processor resulted in operators being unaware of the problem entirely. In an extremely unfortunate coincidence, the utility’s Reliability Coordinator also had computer problems and was lacking the visual tools necessary to provide support.<sup>74</sup> These failures shifted power flows to a system of 138-kV lines which were unable to handle the added current flows, also overloading the last remaining 345-kV path into the area, and beginning the major, uncontrollable cascading sequence.<sup>75</sup> This sequence tripped over 500 generating units and 400 transmission lines in only eight minutes – most of which actually occurred *in the last 12 seconds* of the cascade.<sup>76</sup>

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversary attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying key generation and transmission nodes; altering protective relay settings so that grid components trip off line (or fail to do so) in ways that intensify the outages; denying grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and taking other measures designed to produce cascading failures.<sup>77</sup>

---

<sup>73</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, pp. 1 and 7.

<sup>74</sup> North American Electric Reliability Corporation, *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?*, July 13, 2014, pp. 27-28.

<sup>75</sup> *Ibid.*

<sup>76</sup> North American Electric Reliability Corporation, *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?*, July 13, 2014, p. 109.

<sup>77</sup> Anton Cherepanov and Robert Lipovsky, “Industroyer: Biggest threat to industrial control systems since Stuxnet,” *ESET Blog: WeLiveSecurity*, June 12, 2017, <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat->

Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe – particularly by undermining situational awareness data and capabilities.

The imminent danger or occurrence of adversary-induced cascading outages could be criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt the operation of grid devices and networks essential to CEI and DCEI – and do so on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

As will be discussed in Section III, it may be difficult to determine that an impending attack poses an imminent danger of creating cascading failures given the technical challenges of predicting the systemic effects of cyber and physical strikes. Waiting until an attack is underway to assess the risks of cascades will also pose challenges. As in 2003, failures can spread across vast areas in seconds, and adversaries may seek to disrupt grid operators’ situational awareness. Nevertheless, given the threat that cascading blackouts would pose to CEI and DCEI, any significant risk that adversaries are poised to create such effects should be sufficient to declare a grid security emergency.

Promising opportunities also exist to develop emergency orders to reduce the risk of cascading failures. Emergency load shedding provides one such opportunity. After action reports from the 2003 blackout found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. In particular, a U.S.-Canada task force found that “Timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio.”<sup>78</sup> In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.<sup>79</sup>

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for Transmission Operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation on which to build emergency orders to reduce the risk that physical and cyberattacks will create cascading blackouts, and – potentially – tailor EOs and implementation plans to exclude vital facilities from load shedding.

---

industrial-control-systems-since-stuxnet/; Chris Sistrunk, “ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One),” *SANS Industrial Control Systems*, January 8, 2016, <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>; *United States Computer Emergency Readiness Team*, “Alert (TA17-163A): CrashOverride Malware,” June 12, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-163A>; Dragos, Inc, *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*, June 13, 2017, p. 24.

<sup>78</sup> U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 147.

<sup>79</sup> *Ibid.*, at p. 77.

**c. Uncontrolled Separation.** NERC defines uncontrolled separation as “the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss.”<sup>80</sup> Severe events “resulting in the removal of two or more BES elements with high potential to cascade” can produce uncontrolled separation.<sup>81</sup>

Uncontrolled separation almost always occurs following cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands which “quickly became unstable after the massive transient swings and system separation” because there was insufficient generation within the island to meet electricity demand.<sup>82</sup> Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.<sup>83</sup> In the 1982 West Coast blackout, loss of 500-kV lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, and separation of the system into four unplanned islands.<sup>84</sup> A similar blackout in the same region in 1996 triggered by multiple major transmission line outages, the Western Interconnection again separated into four electrical islands “with significant loss of load and generation.”<sup>85</sup>

Unplanned islands are inherently unstable. Uncontrolled separation only rarely (and near-miraculously) produces synchronous islands in which load and generation are balanced within their perimeters.<sup>86</sup> A better way to produce stable islands may be to pre-plan for them. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, pre-planned islands might become a hedge against cascading failures and uncontrolled separation. In practice, such islanding will entail immense technical and operational problems. Section IV provides a detailed analysis of these opportunities and challenges.

Taken together, these criteria for maintaining grid reliability could constitute “high level” thresholds for declaring GSEs. If the Bulk Power System faced an imminent threat of cascading blackouts, uncontrolled separation, or widespread instability, the potential consequences for the U.S. economy and national security would be so severe that declaration of a GSE should be near-automatic.

However, systemic threats to grid reliability are far from the only criteria that the President might want to consider. Much more narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security – including the National Capital Region – might be

---

<sup>80</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, p. 6.

<sup>81</sup> *Ibid.*, at p. 13.

<sup>82</sup> U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 75.

<sup>83</sup> *Ibid.*, at p. 104.

<sup>84</sup> *Ibid.*, at p. 105.

<sup>85</sup> *Ibid.*, at p. 106.

<sup>86</sup> National Academy of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation’s Electricity System* (Washington D.C.: The National Academies Press, 2017), p. 81.

sufficient to declare a grid security emergency. The President should retain adequate flexibility to make such declaration across a broad range of contingencies. Developing emergency orders to protect and restore service to such critical areas should be a priority as well, together with orders to prevent cascading failures across larger portions of the United States.

### **3. Further Options to Support GSE Declarations: Attack Consequences, Geopolitical Circumstances, and Adversary Efforts to “Prepare the Battlefield”**

Additional criteria can help clarify thresholds for declaring GSEs and for issuing emergency orders while providing such latitude. One criterion is the potential impact of attacks on U.S. national security, the economy, and public health and safety. As noted above, the FPA defined GSEs as occurring when attacks “could disrupt the operation” of CEI or DCEI.<sup>87</sup> Policymakers should consider refining that overly broad standard by leveraging the definition of “significant cyber incidents” in Presidential Policy Directive-41 (PPD-41), *United States Cyber Incident Coordination*. Under PPD-41, “significant cyber incident” are those that are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.”<sup>88</sup> That demonstrable harm standard can help set an appropriately high bar for declaring GSEs and issuing EOs

For determining that attacks are imminent, decision makers might also take the geopolitical climate into account. It is (barely) conceivable that adversaries will launch a “bolt from the blue” attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region, and attack the grid to disrupt the deployment of U.S. forces to the region or achieve other military and political goals.<sup>89</sup> Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause demonstrable harm via grid attacks, should carry greater weight in crises than in peacetime.

The emergence of a regional crisis would also provide opportunities to intensify and specially target searches for destructive malware. Industry and government should ensure that as tensions rise, agencies are already prepared to ramp up intelligence sharing with BPS entities, especially in terms of specific malware signatures to search for in utility networks, data logs, and critical equipment. Pre-attack emergency orders could help facilitate such intensified collaboration.

Gathering and sharing data on adversary efforts to prepare the battlefield can also support GSE determinations. DOE and its industry partners have taken major strides to improve such sharing;

---

<sup>87</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>88</sup> White House, *Presidential Policy Directive - United States Cyber Incident Coordination*, July 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

<sup>89</sup> Section II C examines these national security-related issues and their implications for designing emergency orders.



especially on the operational technology networks (OT) and other systems that help control grid operations. For example, DOE's Cybersecurity Risk Information Sharing Program is a public-private partnership to build bi-directional situational awareness and facilitate classified and unclassified information sharing.<sup>90</sup> The CRISP is managed by the E-ISAC, which plays an integral role in establishing situational awareness in the electricity subsector. The E-ISAC is also central to electric industry incident coordination efforts, including cybersecurity threat assessments and sharing incident data.<sup>91</sup>

Advancing the ability to improve situational awareness of OT networks is a key focus of DOE's current activities. The Department is currently in the early stages of taking the lessons learned from CRISP and developing an analogous capability to monitor traffic on OT networks via the Cybersecurity for the Operational Technology Environment (CYOTE) pilot project. Observing anomalous traffic on networks – and having the ability to store and retrieve network traffic from the recent past – can be the first step in stopping an attack in its early stages.

The President's advisors may want to employ additional technical criteria in making pre-attack GSE determinations. One opportunity lies in using the Industrial Control System (ICS) Cyber Kill Chain, which identifies the specific, sequenced phases that adversaries execute in order to conduct attacks that inflict predictable physical effects on grid equipment and operations.<sup>92</sup> Stage 1 begins with planning and reconnaissance against ICS networks, and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing capabilities to attack ICS networks, and – ultimately – executes the attack. Evidence of an adversary's position along this Kill Chain could help support decision-making on the imminence of potential threats, with the final phases posing the most proximate risks of attack.

Another option lies in using established Federal cyber incident criteria. For example, consistent with PPD-41, *United States Cyber Incident Coordination* (July 2016), the National Cyber Incident Response Plan (NCIRP) issued in December 2016 provides a Cyber Incident Severity Schema to serve as “a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments” and agencies.<sup>93</sup> Appendix A provides the Schema. As efforts go forward to refine the Schema and the NCIRP, significant opportunities will exist to crosswalk and provide for consistency between such Federal Government-wide assessment systems and possible GSE thresholds for internal use by the President and supporting staff and departments.<sup>94</sup>

---

<sup>90</sup> “Energy Sector Cybersecurity Preparedness,” *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

<sup>91</sup> “Electricity ISAC,” *NERC*, n.d.a., <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>92</sup> The ICS Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin in 2011 to “help the decision-making process for better detecting and responding to adversary intrusions.” The ICS Cyber Kill Chain tailors that decision-making tool for ICS-specific cyber threats and consequences. See: Michael Assante and Robert M. Lee, “The Industrial Control System Cyber Kill Chain,” *SANS Institute*, <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.

<sup>93</sup> Department of Homeland Security, *National Cyber Incident Response Plan*, December 2016, pp. 29-30.

<sup>94</sup> One option would be to explicitly link the declaration of a GSE to the designation of a cyber incident as a “Level 5 Emergency,” which poses “an imminent that to the provision of wide-scale critical infrastructure services, national government stability, or to the lives of U.S. persons.” But other Schema levels (either lower, or, potentially, higher if

Of course, an enormous difference exists between making preparations for an attack and actually launching one. But if adversaries were to suddenly move to the penultimate phase of stage 2 (delivery and installation of the attack capability) during an intense political crisis or regional confrontation, evidence that they had taken such a move could help support GSE decision-making. Gathering such evidence against sophisticated attackers may require sustained improvements in sensors and OT/IT system monitoring.

### **C. PRE-ATTACK GSE DECLARATIONS: OPTIONS FOR DATA SHARING AND CONSULTATION WITH INDUSTRY**

Decisions regarding pre-attack GSE declarations would benefit significantly from thorough industry consultation. However, neither the Federal Power Act nor the *Final Rule on Grid Security Emergency Orders: Procedures for Issuance* explicitly provide for such discussions. The GSE Rule specifies that “before an emergency order is put into effect and, to the extent practicable and in light of the nature of the grid security emergency and the urgency of the need for action, efforts will be made to consult” with the ESCC, the owners, users and operators of CEI and DCEI, and other resilience stakeholders.<sup>95</sup> DOE might benefit from making equivalent commitments to seek industry input on the declaration of GSEs.

Only power companies will have access to the precursory malware that adversaries implant on their networks, as well as unique expertise in assessing the potential impact of the malware on their systems if attacks begin. Government leaders should consider consulting with BPS entities before the President declares a GSE so that the President’s advisors can benefit from their technical perspectives, and so that government and industry can jointly prepare for the media turmoil that a declaration will almost certainly produce.

As with consultations on issuing orders, urgent circumstances could foreshorten or preclude opportunities for government dialog with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of “bolt from the blue” attacks. However, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be extraordinarily valuable in determining whether (and when) to declare a grid security emergency. Now is the time to explore options to coordinate such discussions, preferably by leveraging existing consultative mechanisms under the ESCC and E-ISAC.

### **III. A FRAMEWORK FOR DEVELOPING EMERGENCY ORDERS: GSE PHASES AND ORDER DESIGN OPTIONS**

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal with these ambiguities is to delay the

---

additional categories are developed) could provide for such linkages. Department of Homeland Security, *National Cyber Incident Response Plan*, December 2016, p. 38.

<sup>95</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1181.

declaration of a GSE until blackouts begin, foregoing the benefits of issuing pre-attack emergency orders. Industry and government partners should instead explore options to design EOs for the Secretary to issue when risks of cyberattack are elevated – especially if such orders will have little or no disruptive effects on normal grid service. These partners should also develop more extreme and potentially disruptive options for use when attacks are underway and when restoration operations begin.

## **1. Pre-Attack Options**

Conservative operations that utilities implement against natural hazards help illuminate the value that pre-attack EOs could offer against manmade threats. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects, and prepare for possible response and restoration operations if grid infrastructure is damaged.<sup>96</sup> For example, Reliability Coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.<sup>97</sup> Power companies may also cancel non-critical generation and transmission maintenance activities and staff their back-up control centers, critical BPS substations, and other key facilities to set the stage for emergency operations as hurricanes approach.<sup>98</sup>

A key feature of these frequently-used conservative operations (COs) is that they do not disrupt normal service to customers. The negligible impact of these COs on day-to-day service helps make them more viable for a utility to implement when the storm's path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the U.S. coast. Instead, they provide a wide “cone of uncertainty” that becomes increasingly narrow as the hurricane approaches. However, utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other COs. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these COs do not affect normal service to customers enhances the willingness of utility leaders to order their implementation amidst the uncertainty.

---

<sup>96</sup> Conservative operations are not defined in the NERC Glossary of Terms. However, many Reliability Coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken “to implement additional actions to ensure the BES [Bulk Electric System] remains reliable in the face of the additional threats” when “events, conditions, or circumstances may put the [BES] at an increased level of risk, compared to normal operating conditions.” See: PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 3, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>. Similarly, the Western Electricity Coordinating Council, defines Conservative Systems Operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets “Are restricted and managed in order to maintain or the restore reliability of the power system from the negative influence of a triggering event or condition.” See: Western Electricity Coordinating Council, *Conservative System Operations* (training slides, n.d.a.), p. 4, [https://www.wecc.biz/Administrative/ProviderXXX\\_CSO\\_20XX\\_Presentation.pdf](https://www.wecc.biz/Administrative/ProviderXXX_CSO_20XX_Presentation.pdf).

<sup>97</sup> PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 3, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.

<sup>98</sup> PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 9, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.

Industry and government partners should borrow from this model to develop orders for pre-attack conservative operations against cyber and/or physical attacks. As a regional confrontation or other precipitating crisis intensifies, it is possible (though unlikely) that the U.S. intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. Instead, based on evidence gathered on utility networks and other sources, the President may need to declare a GSE when it is still not certain that an attack will occur, in order to ensure that sufficient time exists to implement pre-attack conservative operations.

As with COs that power companies adopt when they are within a hurricane's cone of uncertainty, it will be especially helpful to develop pre-attack emergency orders that will not disrupt day-to-day electric service. If the Secretary issues such orders for BPS entities to adopt COs and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented them – but only if those orders also enable entities to recover the costs of doing so. Section IV of this study examines possible “no regrets” emergency orders for conservative operations. Many of them could order COs similar to those developed for natural hazards. For example, pre-attack EOs might order BPS entities to increase generation reserves and/or re-dispatch resources out of least cost operations, and reimburse those entities for the costs they incur.

Other orders might be threat-specific: i.e., to intensify scrutiny of OT networks for malware. Power companies could implement all such no regrets EOs without cutting off power to customers or creating grid instabilities. DOE and its industry partners must consider the development of such options as a special priority for follow-on engineering and operational analysis. Appendix B contains a preliminary list of options for conservative operations which builds on current utility conservative operations procedures, and adds additional, adversary-specific options.

## **2. Putting Additional “Arrows in the Quiver:” Possible EOs for Extraordinary Circumstances**

Industry and government partners should also develop emergency orders that could offer additional benefits for protecting or restoring reliability, even at the price of disrupting normal electric service. Most such orders would be used only under extraordinary circumstances: that is, when adversaries were poised to cripple the reliable operation of the grid, and the BPS was at severe risk of instability, uncontrolled separation, or cascading failure.<sup>99</sup>

Emergency actions taken against severe natural hazards again exemplify the benefits of developing extraordinary measures for grid security emergencies. The shutdown of grid infrastructure on warning of catastrophic storm surges offers a case in point. During Superstorm Sandy, Consolidated Edison (Con Ed) faced the risk of having critical substations and underground electrical equipment inundated by the worst storm surge in nearly 200 years. If seawater hits systems that are still carrying electricity, catastrophic physical damage will result for transformers and other difficult-to-replace grid components. Consolidated Edison's team

---

<sup>99</sup> This formulation follows the definition of reliable operation in FPA, section 215, 16 U.S. Code § 824o(a)(4).

made the politically difficult decision to prevent such damage by pre-emptively cutting of power to lower Manhattan. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.<sup>100</sup> Moreover, Con Ed limited the disruptiveness of the shutdown by notifying customers hours earlier that the utility might halt service, and by already having plans in place to prioritize the restoration of service to hospitals, water-pumping stations, and other critical facilities.<sup>101</sup>

BPS entities continue to use “shutdown on warning” as an effective tool to avoid equipment damage against severe weather, and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent damage to equipment and speed restoration. Generation owners similarly chose to shut down or evacuated some generating units in the storm’s projected path.<sup>102</sup>

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and HVAC systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

Extraordinary measures designed for cyber and physical attacks may entail even greater risks and uncertainties. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an attack is likely to cause cascading failures and demonstrable harm to the U.S. economy, national security, and/or public health and safety. The potential impact of APTs on reliable grid operations may be difficult to determine until attacks are well underway. Even then, myriad factors (including many that grid operators can influence) will affect the likelihood and scope of potential cascading failures.

Nevertheless, a range of emergency orders could help BPS entities reduce the risk of cascading failures and accelerate the restoration of power if outages occur. These EOs vary in terms of when the Secretary would issue them: 1) when attacks are imminent; 2) when they are underway; and 3) when major blackouts exist, and utilities must prioritize and accelerate power restoration to prevent demonstrable, and potentially catastrophic, harm to public safety, national security, and the economy.

Emergency orders can also vary in terms of the degree of disruption they would inflict on normal electric service (and, in many instances, the specific threats they will be designed to counter). Some EOs, including no regrets orders, will have little or no disruptive impact. Others would

---

<sup>100</sup> Rich Miller, “Con Edison Shuts Off Power in Lower Manhattan,” *DataCenter Knowledge*, October 29, 2012, <http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutdown>.

<sup>101</sup> Scott DiSavino and David Sheppard, “ConEd cuts power to part of Lower Manhattan due to Sandy,” *Reuters*, October 29, 2012, <https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030>.

<sup>102</sup> North American Electric Reliability Corporation, *Hurricane Harvey Event Analysis Report*, March 2018, p. v.



have massive effects but – as in cutting off power during Sandy – would also protect grid reliability against longer term disruption and accelerate the prioritized restoration of power.

Figure 1 illustrates these different categories and examples of possible EOs that would fall within them. The leftmost column includes possible EOs that the Secretary would issue when attacks are imminent. Orders for conservative operations, especially those in the no regrets category, would fall into the lower spectrum of disruption to normal service.

**Figure 1 – Emergency Order Matrix: Examples of EO Designs**

Disruption of Normal Grid Reliability / Service	High	Pre-Planned Islanding	Prioritized Load Shedding	Movement of In-Service Transformers to Higher Priority Locations
	Low	Conservative Operations	Suspension of Wholesale Market Operations	Transportation Support for Replacement Transformers
		Protect Reliability When Attack is Imminent	Protect Reliability When Attack is Underway	Restore Service/Reliability
Grid Security Emergency Response Phase				

***a. Extraordinary Measures for Pre-Attack Protection of Grid Reliability: Islanding as a (Problematic) Example***

Pre-attack options with greater disruptive effects would populate the upper left box. Pre-planned power islanding offers an “in extremis” option that has garnered especially strong industry and government interest over the past few years. Microgrids provide the most familiar type of power island. A growing number of military installations (and a handful of hospitals and universities) have generators and other electric infrastructure on their bases, configured so that if the surrounding grid is at risk of losing power, the installations can separate themselves from the grid and operate independently as a power island.

Microgrids do not offer a “bulletproof,” all-purpose defense against imminent attacks. Cyber adversaries are sure to treat on-base electric infrastructure (including renewable generation assets and other systems) as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas-fired generators, the power they provide is only as resilient as

the gas transmission and distribution systems that supply them -- and cyber threats to natural gas systems are rapidly escalating.<sup>103</sup> Moreover, building microgrids requires extensive investment in grid infrastructure – especially if bases want to provide power not only to critical loads within their perimeters, but also for the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to traditional microgrids, power companies have also explored other means of establishing power islands when severe disruptions are imminent. Participants of GridEx, the electric industry’s premier exercise series, have extensively discussed one option that provides an especially useful basis for developing possible pre-attack emergency orders. GridEx participants note that it might be possible to pre-plan to establish large power islands by using existing grid infrastructure within their boundaries. On warning of an imminent attack or under other extraordinary circumstances, power companies would separate the power island from the surrounding grid and operate independently to serve the critical loads within it.

However, strategic islanding will only be practical if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for pre-planned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands. Moreover, standing up islands would severely disrupt day-to-day service for non-critical customers, and create instabilities for surrounding systems that could produce additional service disruptions, economic disruption, and societal unrest. Accordingly, strategic islanding might be considered a “huge regrets” emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created. Further studies will need to examine different models for pre-planned islanding, examines the design and operational challenges they would entail, and analyzes additional pre-attack options for emergency orders.

### ***b. Extraordinary Measures when Attacks are Occurring***

Emergency orders for attacks that are underway could entail similar variation in the degree to which they will disrupt normal service. The lower box in the center column of Figure 1 provides an example of a low-disruption emergency order: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate, “real time” needs or for the next day). These entities have taken extensive measures to keep these market functions separate from their operational control of the grid. Nevertheless, cyberattacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, crush the valuation of power companies on Wall Street, and magnify the damage to the U.S. economy that attacks on the grid will create.

---

<sup>103</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation’s Electricity System: Second Installment of the QER*, January 2017, p. 7-7; Paul W. Parfomak, “Pipelines: Securing the Veins of the American Economy,” *Testimony Before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*, April 19, 2016, pp. 2-3, <http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf>.

RTOs are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the Transmission Operator<sup>104</sup> for the Mid-Atlantic and other U.S. regions, has called for the development of mechanisms to permit “non-market” operations in extreme circumstances.<sup>105</sup> A number of options exist to provide for such operations. For example, if the Secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell power at a fixed price pre-determined by DOE.<sup>106</sup> Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high benefit/low disruption emergency orders examined later in this study, including orders for maximum power generation when attacks are underway, will also fall into this category.<sup>107</sup>

Utilities are already beginning to develop tools and procedures to support extraordinary operations, which DOE and industry can leverage in EO development efforts. The ESCC, for example, has led a focus on exploring how entities may operate the grid “under sub-optimal circumstances,” to ensure that these entities can anticipate, plan for, and practice using extraordinary measures to do so.<sup>108</sup> Notably, this includes the North American Transmission Forum’s “Spare Tire” program, launched in 2016, which is exploring how entities may operate the BES without primary and backup control centers.<sup>109</sup>

---

<sup>104</sup> The NERC Glossary defines Transmission Operator as: “The entity responsible for the reliability of its local transmission system, and that operates or directs the operations of the transmission Facilities.” Transmission Operator Area is defined as: “The collection of Transmission assets over which the Transmission Operator is responsible for operating.” See: “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

<sup>105</sup> PJM Interconnection, LLC, “COMMENTS AND RESPONSES OF PJM INTERCONNECTION, L.L.C.,” *In Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000), March 9, 2018, pp. 6 and 39-40.

<sup>106</sup> Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. *Ibid.*, at p. 39.

<sup>107</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see: MISO, “MISO January 17-18 Maximum Generation Event Overview” (slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018), <https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf>.

<sup>108</sup> “ESCC,” *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.

<sup>109</sup> “North American Transmission Forum External Newsletter,” *North American Transmission Forum*, January 2018, <https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf>. For more information on NATF’s Spare Tire program, see: North American Transmission Forum, *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—a Spare Tire Approach*, 2017, <http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf>.

Industry and government partners will also need to develop more disruptive EOs that can protect grid reliability in extraordinary circumstances. The top center box of Figure 1 provides a case in point: prioritized load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by shedding load – most often by implementing rotating blackouts.<sup>110</sup>

Grid operators used load shedding to protect grid reliability during the “Big Chill” that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT initiated controlled rolling blackouts during the event that affected a total of 4.4 million customers over the course of the event.<sup>111</sup> Those temporary blackouts were no doubt disruptive, especially for customers with electric heating systems. However, by reducing the risk of cascading failures, load shedding offered compelling system-wide benefits for protecting reliability.

Industry and government partners could develop emergency orders for load shedding to protect grid reliability during cyber and/or physical attacks. If adversaries are able to inflict deep, multi-region losses in generation and transmission resources, load shedding will offer an essential tool to prevent broader grid instabilities – albeit at the price of disrupting normal service to many millions of customers. NERC already requires BPS entities to have plans for load shedding.<sup>112</sup> In the EO design process, industry and government can build on that foundation to not only protect against cascading failures, but also prioritize load shedding so as to sustain service to facilities critical for national security, the economy, and public health and safety.

### ***c. Emergency Orders to Support Power Restoration***

The rightmost column in Figure 1 provides the third category for emergency orders: EOs that can help grid owners and operators restore power after widespread outages occur. In past cascading failures of the U.S. electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days or less because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators,

---

<sup>110</sup> North American Electricity Reliability Corporation, *Severe Impact Resilience: Considerations and Recommendations*, May 9, 2012, p. 11.

<sup>111</sup> FERC and NERC, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*, January 2016, p. 61.

<sup>112</sup> NERC standards currently emphasize automatic load shedding to protect grid reliability. See: NERC, *PRC-006-3 – Automatic Underfrequency Load Shedding*, effective October 1, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States); and NERC, *PRC-010-2 – Under Voltage Load Shedding*, effective April 2, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States). However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing EOs to prevent or mitigate cascading failures. See: NERC, *EOP-011-1 Emergency Operations*, effective April 1, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).

transmission lines, and other system components are designed to trip off line when instabilities occur, thereby protecting them from being damaged by power surges – and leaving them available to help rapidly re-establish the flow of power.<sup>113</sup>

However, if cyber or physical attacks destroy transformers and other critical system infrastructure, requirements to repair or replace such assets could greatly lengthen and complicate restoration operations. BPS entities already have detailed plans to restore power and, as circumstances dictate, prioritize the restoration of service to nuclear power plants and other critical customers. Industry and government should consider developing emergency orders that build on these existing plans and capabilities, and prioritize restoration for a wider array of CEI and DCEI – even if adversaries inflict unprecedented physical damage on grid components.

One option for restoration orders includes ordering utilities to operate in an N-0 operating state, unless one contingency would cause cascading failures. Currently, NERC standards require BPS entities to operate in an N-1 state: they are able to handle the most severe single contingency ('N-1').<sup>114</sup> Operators may be required to shed load to maintain the N-1 state. However, returning to an N-1 state after a major outage is likely to be a lengthy process, involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. If the Secretary were to order utilities to operate at N-0 as needed, they could do so without facing punishment for violating NERC standards. Creating such an option would provide greater operating flexibility and ensure that entities can continue to serve as much load as possible. Entities would only be required to shed load for the most severe single contingency if that single contingency would cause cascading failures or following a contingency that required load shedding to eliminate overloads or low voltage.

Restoration EOs should also account for the risk that adversaries will continue their attacks as power companies begin restoring service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to U.S. military bases and other vital facilities, and seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeted against power restoration operations can help achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply.

The Department of Defense can play a vital role in preventing such attacks. If directed by the President, United States Cyber Command (USCYBERCOM) and other DOD components would do their utmost to “shoot the archer,” and prevent the adversary’s cyber forces from launching further strikes on the grid and other U.S. targets. But re-attacks may nevertheless occur. For example, unless power companies thoroughly scrub advanced persistent threats already hidden

---

<sup>113</sup> NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, December 2010, p. 1. See also: U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 8.

<sup>114</sup> North American Electric Reliability Corporation, *BAL-002-2(i) – Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event*, Requirement R2, effective January 1, 2018.



their networks, those APTs may launch repeated re-attacks against the grid and create recurring outages.<sup>115</sup> Physical attacks to disrupt restoration operations, including against replacement transformers being moved to critical substations, would create additional challenges.<sup>116</sup>

As with EOs for imminent and ongoing attacks, emergency orders to accelerate power restoration will differ in their disruptiveness to normal grid operation. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks and barges) from where power companies store them to where they are needed as replacements.<sup>117</sup> The Secretary has no authority under the Federal Power Act to issue orders to transportation sector assets. However, in collaboration with the Department of Transportation, rail and other asset owners, and SLTT transportation agencies, DOE and the private sector could pre-plan to waive transportation regulations, inspection requirements, and other potential impediments on a nationwide basis. Such plans could also be structured to help protect transportation operations against active shooters or other attacks.

EOs could also be created for *in extremis* restoration operations that would more sharply depart from existing industry plans and procedures. As the starting point for that development process, power companies and their government partners might assume that attacks will not be “one and done,” but instead be part of a sustained campaign in which adversaries will single out restoration operations for disruption. An example of *in extremis* orders: if adversaries managed to damage or destroy an extraordinarily large number of transformers, the Secretary might order that surviving, in-service transformers in the same voltage class be removed from their substation and transported to serve vital national security facilities in the National Capitol Region or other areas. Such orders could create severe disruptions in existing service. However, the benefits might be greater still for helping the United States defeat its adversary.

### **3. Next Steps in the EO Development Process**

Potential emergency orders differ not only in terms of the phases of an attack in which they would be most useful, and in their mix of benefits and disruptive impact on normal grid operations, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create – especially those that fall into the “no regrets” category. As noted above, utilities frequently use COs to help protect grid reliability in severe weather events, and a growing number of companies are already building on that foundation to draft equivalent COs against cyber and physical threats.<sup>118</sup> Emergency orders based on those initiatives constitute “low hanging fruit;” creating such orders offers an immediate opportunity

---

<sup>115</sup> Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee: Part I – Incident Response*, June 2016, p. 7.

<sup>116</sup> The GridEx exercise series accounts for physical attacks that disrupt restoration operations. See: NERC, *Grid Security Exercise: GridEx III Report*, March 2016.

<sup>117</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, pp. 12-13, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>118</sup> PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 54.

for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging EO initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are underway, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. The next step to do so is to examine how emergency orders can be framed to reflect and achieve specific U.S. security priorities and meet the other development requirements that they will entail.

#### **IV. ADDITIONAL EMERGENCY ORDER DESIGN PARAMETERS AND SUPPORTING INITIATIVES**

The U.S. *National Security Strategy* provides crucial guidance on how emergency orders can help deter attacks on the grid and other U.S. targets, and how those orders can help the United States defeat adversaries if deterrence fails. However, DOE and BPS entities will also need to overcome the immense communications challenges that the use of emergency orders will entail, including requirements to explain to the U.S. public why extraordinary measures are being employed and what they should expect if attacks continue. Incorporating provisions for regulatory waivers and cost recovery in the design of template emergency orders will offer compelling advantages as well.

##### **A. DETERRING AND DEFEATING U.S. ADVERSARIES**

Adversaries will strike the U.S. grid not merely to cause blackouts, but as a means to help them achieve their broader political, economic, and military objectives against the United States. Government and industry partners should design emergency orders to help prevent attackers from accomplishing their objectives, and – ideally – help deter them from attacking at all.

The U.S. *National Security Strategy* offers an overarching framework to guide such design efforts. The *Strategy* emphasizes that cyber threats to U.S. critical infrastructure are becoming increasingly severe, and notes that cyber weapons “enable adversaries to attempt strategic attacks against the United States – without resorting to nuclear weapons – in ways that could cripple our economy and our ability to deploy our military forces.”<sup>119</sup> To counter these threats, the *Strategy* identifies two essential priorities, both of which emergency orders can be designed to support:

- Deter adversaries from attacking by convincing them they will suffer “swift and costly consequences” and be defeated if they strike the grid or other U.S. targets;<sup>120</sup>
- Strengthen infrastructure resilience to make adversaries doubt that “they can achieve their objectives” if they do attack (i.e. deterrence by denial).<sup>121</sup>

---

<sup>119</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 27.

<sup>120</sup> *Ibid.*, at p. 28.

<sup>121</sup> *Ibid.*, at p. 13.

## **1. Deterrence through Threats of Punishment and Defeat: Implications for Emergency Order Design**

One important way that emergency orders can strengthen deterrence is by helping convince adversaries that the United States will be able to effectively respond to attacks and impose consequences that those adversaries would consider unacceptable. A relatively small number of U.S. military bases are responsible for conducting such response operations. The U.S. Defense Science Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of U.S. strike systems (cyber, nuclear, and non-nuclear) and supporting infrastructure to ensure “that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyberattacks.”<sup>122</sup> Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should and immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which U.S. strike systems rely and ensure that they have reliable power for however long a conflict might continue.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The *Strategy* emphasizes that “We must convince adversaries that we can and will defeat them – not just punish them if they attack the United States.”<sup>123</sup> As noted in Section II, adversaries are most likely to attack the grid in the context of an intense regional confrontation with the United States and its allies in the South China Sea, the Baltics, or some other crisis abroad. A vast array of U.S. Defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy and sustain U.S. power projection forces for regional contingencies. Ensuring the availability of resilient power for these essential facilities and functions will require the development of emergency orders to serve a greatly expanded set of customers than for U.S. strike systems alone, and encompass a much larger array of DCEI owners and operators.

Emergency orders and implementation plans will need to account for a further challenge: the risk that adversaries will selectively target defense critical electric infrastructure and prioritize its disruption through especially sophisticated cyber and physical attacks. The Department of Defense (DOD) *Mission Assurance Strategy* (2012) emphasizes the growing risk that adversaries will seek to degrade U.S. military capabilities by attacking the infrastructure on which DOD depends. In particular, “Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting critical Defense and supporting civilian capabilities and assets,” including the U.S. power grid.<sup>124</sup>

---

<sup>122</sup> James N. Miller and James R. Gosler, “Memorandum for the Chairman, Defense Science Board” (preamble), *Task Force on Cyber Deterrence*, February 28, 2017. See also: Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, pp. 3, 6-7, 11-12, and 17-18.

<sup>123</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 28.

<sup>124</sup> Department of Defense, *Mission Assurance Strategy*, April 2012, p. 1, [http://policy.defense.gov/Portals/11/Documents/MA\\_Strategy\\_Final\\_7May12.pdf](http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf).

Electric companies and Defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds to serve Defense installations provides a valuable means of strengthening resilience.<sup>125</sup> Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.<sup>126</sup> And, as briefly discussed in Section II, utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as “power islands” independent of the surrounding grid.<sup>127</sup>

While valuable, these initiatives do not eliminate the need to develop Defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases. Emergency generators will break down in long duration outages, and resupplying them with fuel will become increasingly difficult at installations that lack massive storage tanks. Large-scale microgrids for islanded operations can provide more resilient power; DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for warfighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, ranging from the water utilities and other “outside the fence” infrastructure that support base operations, to the intermodal transportation systems that help deploy and sustain U.S. forces abroad.

Emergency orders can help support deterrence and power projection far more quickly and with less infrastructure investment. Over the past year, the Department of Defense has been collaborating with power companies and DOE to develop new emergency measures to protect the resilience of electric service to military bases by prioritizing the flow of power to bases when generation capacity falls short of total load, and through other emergency operations. BPS entities are also launching initiatives with DOD and DOE to ensure that power to Defense installations can be restored far more rapidly than is possible today if adversaries create wide-area blackouts.<sup>128</sup>

---

<sup>125</sup> Department of Defense (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment), *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*, July 2017, p. 39, <https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf>.

<sup>126</sup> *Ibid.*, at 40.

<sup>127</sup> *Ibid.* at 39. See also: Lincoln Laboratory, *Microgrid Study: Energy Security for DoD Installations* (Technical Report 1164), June 2012, <https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf>; and Pew Charitable Trusts, *Power Begins at Home: Assured Energy for U.S. Military Bases*, January 12, 2017, pp. 13-15. A number of “islandable” microgrid projects are underway at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See: Michael McGhee, “EEI Executive Advisory Committee,” (slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017), p. 4, [http://www.asaie.army.mil/Public/ES/oei/docs/EEI\\_Exec-Committee.pdf](http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf); and Cheryl Kaften, “DoD Tests Energy Continuity with ‘Islanded’ Microgrid,” *Energy Manager Today*, April 5, 2017, <https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/>.

<sup>128</sup> “Rapid Attack Detection, Isolation and Characterization Systems (RADICS),” *Defense Advanced Research Projects Agency*, n.d.a., <https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems>.

These initiatives provide an increasingly robust foundation for developing emergency orders to reinforce U.S. deterrence and power projection capabilities. For protection against imminent attacks, it may be possible for power companies to develop plans for conservative operations that are specially targeted to protect the defense critical electric infrastructure in their service areas. Pre-planned islanding could provide unique benefits for military bases and supporting systems (though only if power companies can overcome the immense technical and operational impediments such islanding entails). The development of EOs and company-specific implementation plans for prioritized load shedding, in extremis restoration support, and other potential orders also offer additional opportunities to build on industry-government collaboration already underway for post-attack emergency operations.

The prerequisite for these development efforts will be for the Secretary to identify which military bases and supporting assets are most critical to protect. Section 215A of the Federal Power Act provides a starting point to do so. The Act requires the Secretary of Energy, in consultation with other Federal agencies and grid owners and operators, to identify and designate “critical Defense facilities” in the 48 contiguous states and the District of Columbia that are “1) critical to the defense of the United States; and 2) vulnerable to a disruption of electric energy provided to such facility by an external provider.”<sup>129</sup> Congress also created a definition of *Defense Critical Electric Infrastructure* (DCEI) to help guide implementation of that requirement. DCEI constitutes “any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]” as a critical Defense facility, “but is not owned or operated by the owner or operator of such facility.”<sup>130</sup>

The Department of Energy is already working with the Department of Defense to identify and strengthen the resilience of power flows to critical Defense facilities. DOE is also already working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate infrastructure identified as DCEI. Fortunately, DOD already has a well-established, continuously-updated list of Defense Critical Infrastructure (including military bases and other assets) to help provide input to DOE.<sup>131</sup> A wide variety of factors contribute to determining the criticality of a particular military base or other Defense asset. However, for designing emergency orders that help achieve the deterrence and defense priorities of the *National Security Strategy*, priorities for protecting and restoring service fall into three categories. Figure 2 depicts these categories as a set of concentric circles.

## Figure 2 – Categories for Protecting Defense Critical Electric Infrastructure

---

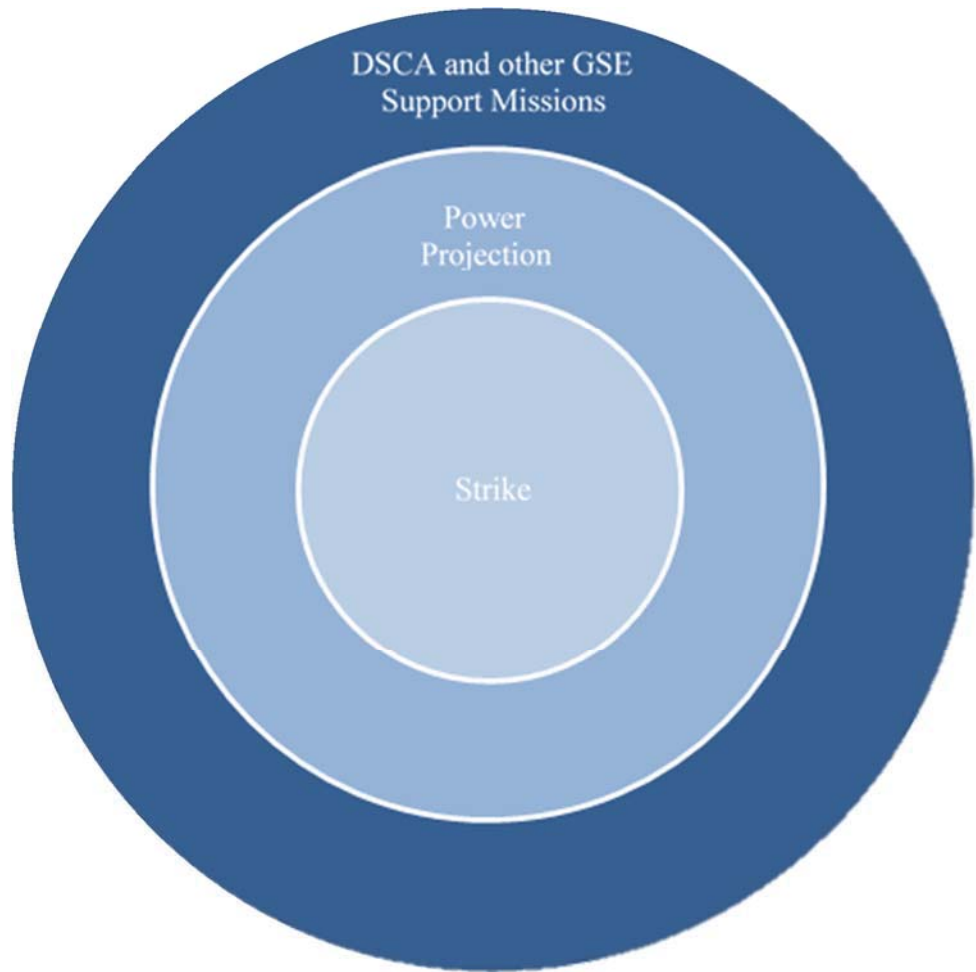
<sup>129</sup> 16 U.S.C. § 824o–1, Section (c), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>130</sup> 16 U.S.C. § 824o–1, Section (a)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>131</sup> See: Department of Defense, *Department of Defense Manual 3020.45: Defense Critical Infrastructure Program (DCIP): Execution Timeline*, last updated May 23, 2017, <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>; and Department of Defense, *Department of Defense Directive 3020.40: Mission Assurance (MA)*, November 29, 2016, [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).



At the innermost core lies those installations and supporting infrastructure that are essential for inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital; protecting the reliability of the DCEI on which they depend is crucial and should be the top priority for developing emergency orders and company-specific implementation plans.



The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining them abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the U.S. grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. The Department of Defense is in the process of identifying the specific facilities and supporting infrastructure that is required to help execute Operational Plans (OPLANS) around the globe.<sup>132</sup> DOD also has well-established criteria and assessment methods to prioritize these supporting assets for risk-mitigation.<sup>133</sup> These tools should be used to identify the broader set of defense critical electric infrastructure needed for deterrence, and to help power companies pre-plan to support critical assets within their service footprints.

---

<sup>132</sup> Department of Defense, *Department of Defense Directive 3020.40: Mission Assurance (MA)*, November 29, 2016, [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).

<sup>133</sup> Department of Defense, *Department of Defense Manual 3020.45: Defense Critical Infrastructure Program (DCIP): Execution Timeline*, last updated May 23, 2017, <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>

The third circle includes the still larger array of Defense installations, including National Guard bases, which would be essential for providing Defense Support to Civil Authorities (DSCA) if disruptions of the grid jeopardize public health and safety. In Hurricane Maria (2017), superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and providing other assistance. Protecting or rapidly restoring the reliability of the DCEI that supports these DSCA functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public. Ultimately, however, countering such adversary efforts will require protecting grid service to the still broader array of hospitals, water systems, and other civilian assets served by critical electric infrastructure.

## **2. Deterrence by Denial: Protecting Critical Electric Infrastructure**

Emergency orders can also strengthen deterrence through a very different means. In addition to deterring adversaries by threatening to inflict unacceptable costs if they attack, and being able to defeat them abroad if war occurs, the United States can also discourage attacks by making adversaries doubt that those attacks can inflict major disruptions on the grid. The *National Security Strategy* notes that “A stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.”<sup>134</sup> Bolstering such “deterrence by denial” constitutes a prime goal for developing emergency orders, as well as a source of challenging design requirements.

A special advantage of deterrence by denial is that it does not rely on attack attribution to discourage adversaries from striking the grid. Threats to impose unacceptable costs on attackers will only work if adversaries believe that the United States will be able to identify them as the perpetrators. To evade punishment, attackers are likely to take extraordinary technical measures to complicate or defeat such attribution. The Federal Bureau of Investigation and other Federal agencies need to continue strengthening their attribution capabilities accordingly.<sup>135</sup> FPA information sharing mechanisms can support such improvements by helping speed and secure the delivery of malware samples and other threat signature information between utilities and government agencies.<sup>136</sup>

Nevertheless, despite these efforts, sophisticated adversaries may still doubt whether the United States will be able to identify them as the attacker. Emergency orders that bolster grid resilience can support a different means to deter these adversaries. By helping power companies sustain service to essential customers, emergency orders can heighten adversary doubts as to whether

---

<sup>134</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 13.

<sup>135</sup> Scott S. Smith, “Roles and Responsibilities for Defending the Nation from Cyber Attack,” *Testimony Before the Senate Armed Services Committee*, October 19, 2017. See also: Lily Hay Newman, “Hacker Lexicon: What is the Attribution Problem?,” *WIRED*, December 24, 2016, <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.

<sup>136</sup> See: 16 U.S.C. § 824o–1, Section (d), <https://www.law.cornell.edu/uscode/text/16/824o-1>. Later sections of this study provide a more detailed assessment of provisions for improved information sharing.

attacks will be effective and reduce the expected benefits of striking the grid regardless of U.S. attribution capabilities.

Orders that contribute to deterrence by denial will also be useful against adversaries who do not care that the United States will punish them for attacks on U.S. critical infrastructure. For threats of cost imposition to work, the United States must be able to identify and destroy things that foreign leaders would find intolerable to lose.<sup>137</sup> However, it will be very difficult to target anything that leaders of the Islamic State would find so precious.<sup>138</sup> Deterring cyberattacks through threats of punishment could also be difficult against leaders such as Kim Jong Un.<sup>139</sup> Emergency orders can provide an alternative means to discourage these adversaries from attacking the grid by reinforcing their doubts that they can achieve the disruptive effects they seek.

Finally, emergency orders and the improvements in grid resilience they provide could help U.S. leaders prevail in future confrontations. In regional conflicts that have not yet escalated to full-scale cyberattacks attacks against the United States, U.S. leaders may wish to launch carefully-selected strikes (via cyber or conventional means) against adversaries to encourage them to de-escalate and negotiate for peace. Those leaders may be reluctant to employ strike options if they believe adversaries could cripple the U.S. grid in response. By strengthening the confidence of the President and his advisers that the grid can survive attack(s), and sustain service to essential facilities and functions, emergency orders can help widen the range of options available to the President to resolve future conflicts.<sup>140</sup>

Emergency orders will need to meet stringent design requirements to achieve these goals. To strengthen deterrence by denial, and – if deterrence fails – help ensure that the United States will prevail in a conflict, a large and exceptionally diverse set of customers will need resilient power.

---

<sup>137</sup> Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 3.

<sup>138</sup> Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 4; Brian Michael Jenkins, “Countering al-Qaeda: The Next Phase in the War,” *RAND*, September 8, 2002, <https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html>.

<sup>139</sup> Egle Murauskaite, “North Korea’s Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment,” *38 North (US-Korea Institute at Johns Hopkins SAIS)*, September 12, 2014, <http://www.38north.org/2014/09/emurauskaite091214/>. In contrast, James Andrew Lewis argues that “the primary objective of the North Korean state and the Kim family is regime survival” and they will be loath to put that survival at risk by striking the U.S. grid and other critical infrastructure. James A. Lewis, “North Korea and Cyber Catastrophe—Don’t Hold Your Breath,” *38 North (US-Korea Institute at Johns Hopkins SAIS)*, January 12, 2018, <http://www.38north.org/2018/01/jalewis011218/>. On the broader challenges of tailoring threats of punishment to deter specific nations and foreign leaders, see Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 12.

<sup>140</sup> Even if the United States greatly strengthens grid resilience, the use of cyber weapons in future conflicts will be fraught with risks of rapid (and perhaps unintended) escalation. Jim Miller and Richard Fontaine argue that structural incentives exist for rapid escalation in cyberspace, and that adversaries will have incentives to employ cyber capability “in large doses early in a major conflict to gain coercive and military advantage – and to attempt to prevent the other side from gaining such an advantage.” Miller and Fontaine, *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies are Reshaping Pathways to Crisis and Conflict*, September 2017, p.16.

See also: Jason Healy, “The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities,” *Columbia University*, June 2016, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2836206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206).

Only a limited set of military bases and supporting civilian assets are critical to the defense of the United States. However, adversaries may seek to not only disrupt U.S. Defense capabilities, but also jeopardize societal continuity by crippling electric service to regional hospitals, major financial institutions, and other facilities essential to the U.S. economy and public health and safety.

### **3. Building a “Section 9+ List:” Prioritizing Infrastructure for Sustainment and Restoration**

The Federal Power Act emphasizes the need to protect and restore CEI which, if destroyed or incapacitated, would “negatively affect” national security, the U.S. economy, and public health or safety. But such effects could result from the loss of power to many thousands of hospitals, water utilities, communications systems, and other assets spread across all 16 critical infrastructure sectors. Industry and government do not have the operational resources required to sustain and rapidly restore all critical infrastructure that may be impacted by a large-scale attack.

DOE and its private sector partners will therefore need to pre-identify a far more specific and stringently-prioritized list of critical assets and supporting CEI to protect. To develop template emergency orders and contingency plans to implement them, industry and government will need to determine which specific customers (and the critical electric infrastructure that serves them) are the most critical recipients of prioritized power flows if normal service breaks down.

Executive Order 13636 (February 2013) provides the best methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the Secretary of Homeland Security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.”<sup>141</sup> That standard – catastrophic damage – provides a basis to identify the highest priority assets and associated CEI for protection by emergency orders in GSEs. Over time, orders and contingency plans could gradually encompass less critical facilities and grid infrastructure.

Of course, the Section 9 methodology and subsequent list were never intended to support the implementation of Section 215A of the FPA. As a result, the Section 9 methodology falls short of meeting all the requirements for supporting emergency order design. This methodology, for example, is designed specifically for cybersecurity incidents. Meanwhile, the FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on critical grid assets. EO 13636’s Section 9 requirements also create a “corporate” level list that is not broken down to the key priorities within the corporation (i.e., facilities, systems, and nodes). Identifying the most critical assets and facilities as priorities in GSEs will require a more fine-grained analysis which considers the increasingly complex interdependencies of U.S. critical infrastructure.

---

<sup>141</sup> Executive Order 13636 – *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

Despite these shortfalls, DHS' Executive Order 13636 methodology can provide a valuable starting point for identifying the most vital CEI and supporting assets. DOE and its industry partners should leverage that methodology to create a "Section 9+" list, tailored to fulfill FPA emergency order requirements. Other government efforts to prioritize critical infrastructure, could also make valuable contributions to the list and overall prioritization effort.<sup>142</sup> However, further impediments exist to ensuring that such a list will be effective.

The Section 9 methodology, for example, lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the Federal government tells grid owners and operators if they are on the Section 9 list, they are rarely informed about the Section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data. The Federal government will therefore face inherent problems in building a list of the most critical infrastructure assets and components nationwide.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that individual pharmaceutical distributors, suppliers of water system treatment chemicals, and other companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations in one industry can produce unintended and unforeseen effects on overall system resilience. Yet, companies have powerful incentives to resist sharing such business-sensitive, proprietary information. Public sector leaders will therefore have to strengthen their industry counterparts' confidence that government agencies would not use this data for regulatory compliance, antitrust, or other purposes not explicitly approved through industry-government dialog.

---

<sup>142</sup> There are numerous examples. DHS' National Critical Infrastructure Prioritization Program (NCIPP) aims to identify "nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance." See: DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, p. 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on "lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity." *Ibid.*, at p. 30. Despite its focus on terrorist threats, HSPD-7 also requires the Secretary of Homeland Security to identify and prioritize systems and assets, which, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. DHS, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, <https://www.dhs.gov/homeland-security-presidential-directive-7>. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the "loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States" and lower jurisdictions. The national level priorities on this list could also be helpful. Section (a)(2), 6 U.S.C. § 1241 – *National asset database*, <https://www.law.cornell.edu/uscode/text/6/1241>.



Securing and containing the distribution of this classified data will also be a crucial consideration. The Section 9+ list or equivalent prioritization efforts, if obtained by adversaries, would serve as an instructive guide on how to maximize the devastation of U.S. critical infrastructure and provide a strategic roadmap for attack. To ensure the Section 9+ list's utility in enabling planning and order design, however, essential efforts to protect this data must be complemented by an improved scheme for providing the data to appropriate individuals (with the required security clearance).

## **B. COMMUNICATIONS REQUIREMENTS FOR ISSUING AND EMPLOYING EMERGENCY ORDERS**

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phone and other normal means of communication fail. Under the Electricity Subsector Coordinating Council (ESCC), they have also built an extensive set of “playbooks” to help companies decide what to tell customers about the incident, and to create “unity of messaging” between government officials and industry representatives on estimated times of restoration (ETRs) and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. In anticipation of attacks causing grid security emergencies, these partners have the opportunity to focus on three specific challenges: 1) maintaining survivable communications systems for issuing and sustaining the implementation of emergency orders; 2) preventing adversaries from gaining access to sensitive emergency orders and classified information; and 3) determining what to say to the U.S. public about the attack, potentially including strategies for countering adversary efforts to intensify public panic and incite disorder.

Requirements for survivable and secure communications will be widely shared across many types of grid security emergencies and template EOs. The section that follows offers recommendations to help meet these common needs. In contrast, for informing the U.S. public as to why the Secretary has issued emergency orders and what customers should expect, “no regrets” conservative operations will generate only minor challenges compared to prioritized load shedding and other orders that disrupt normal service. Pre-planning for such “strategic messaging” will be vital to counter the political leverage that adversaries will seek by attacking the grid and should be an integral part of the emergency order design process.

### **1. Communications Requirements in Grid Security Emergencies**

As with the phases of grid security emergency declarations (starting when attacks are imminent), the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Pre-attack

consultations constitute the initial stage. The Federal Power Act specifies that before the Secretary issues EOs, DOE will consult with power companies and other BPS stakeholders “to the extent practicable...regarding implementation of such emergency measures.”<sup>143</sup> This study also recommends that Federal officials consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The Final Rule on *Grid Security Emergency Orders: Procedures for Issuance* clarifies how DOE’s Office of Electricity Delivery and Energy Reliability (OE) will consult on EOs. The GSE Rule specifies that, if practicable, the Electricity Information Sharing and Analysis Center (E-ISAC) is one of the organizations with which the Secretary will consult. Such consultations will be especially useful for sharing data (including classified data) on attacks that are imminent or underway. The GSE Rule also notes that OE will consult with the Electricity Subsector Coordinating Council (ESCC). The ESCC will provide an especially valuable source of industry perspectives on GSE declarations and EOs because the Council represents all components of the electricity subsector and has extensive experience in coordinating industry incident response operations. In addition, the GSE Rule states that “efforts will be made” to consult with NERC, regional entities such as Regional Transmission Operators, “owners, users or operators” of CEI and DCEI, appropriate Federal and state agencies, and other grid reliability stakeholders.<sup>144</sup>

Issuing emergency orders constitutes the second stage. The GSE Rule states that DOE will “communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances.”<sup>145</sup> However, DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.<sup>146</sup> Doing so will be much more efficient and effective than creating a separate, unfamiliar system for communicating emergency orders. Using established communication systems also has the added benefit of pre-existing legitimacy, which can help DOE and utilities avoid potential questions over authentication and possible adversary attempts to spoof EOs. Industry should provide recommendations to DOE on how best to communicate orders to BPS entities to ensure they will be effectively implemented.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders and monitor their compliance with those EOs. Attacks on the grid are unlikely to be “one and done.” As adversaries continue to try to create grid instabilities, and power companies respond with emergency operations to prevent cascading failures, maintain service to critical facilities, and restore power while under attack, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional EOs and response activities – potentially on a nationwide basis. Reliability Coordinators (RCs) will be a critical touchpoint between DOE and individual

---

<sup>143</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1774

<sup>144</sup> *Ibid.*, at p. 1181.

<sup>145</sup> *Ibid.*

<sup>146</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177

BPS entities. RCs can serve as a focal point between DOE and other government leaders and the BPS entities which are in their purview.

Sustained communications will also be necessary to meet an additional requirement of the Federal Power Act: enforcement of emergency orders. The GSE Rule specifies that “Beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order.”<sup>147</sup> Moreover, “in accordance with available enforcement authorities, the Secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order.”<sup>148</sup>

## **2. Survivability of Communications**

Adversaries will have compelling incentives to combine attacks on the grid with strikes against U.S. communications systems. The 2015 attack on Ukraine’s electric system illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone system; the latter attack prevented customers from reporting outages and disrupted the ability of grid operators to focus on restoration operations accordingly.<sup>149</sup> In turn, if adversaries can lengthen power outages by disrupting communications systems essential for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually-reinforcing disruptions in both sectors.

We should assume that adversaries will attack to maximize these failures, especially since they would already be facing the risk of U.S. response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry-government coordination in grid security emergencies.

The likelihood of such combined attacks will intensify as DOE and its partners move through the sequential communications stages of grid security emergencies. Risks will be lowest in the consultation phase. That is fortunate. Under the ESCC, the electric industry has created extensive mechanisms to coordinate response operations by multiple power companies and coordinate mutual assistance operations with DOE and other government agencies. Consultations on possible emergency orders will leverage that existing ESCC system.

To date, however, ESCC consultations on response operations have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to

---

<sup>147</sup> *Ibid.*, at p. 1182.

<sup>148</sup> *Ibid.*

<sup>149</sup> “Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure,” *ICS-CERT*, February 25, 2016, <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.

distributed denial of service (DDoS) attacks and a range of other increasingly severe threats,<sup>150</sup> as well as the communication sector's reliance on grid-provided electricity (especially in long duration outages that put emergency power assets at risk).

The GSE Rule notes the Department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include "essential actions" to protect bulk power system reliability which require recipients to respond as defined in the alert.<sup>151</sup> DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across the bulk power system. NERC already distributes alerts broadly to users, owners, and operators of the bulk power system in North America. Hence, for issuing emergency orders, the alert system provides DOE with an opportunity for "one stop shopping." The Secretary could issue an order to NERC for distribution to both regional operating organizations (RTOs, ISOs, Reliability Coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is e-mail-based.<sup>152</sup> As a result, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also only includes those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for sustaining power to critical facilities and for implementing emergency orders for prioritized load shedding and other actions.

Industry and government partners should consider additional measures to bolster that alert system or create fallback options for the Secretary to issue orders when attacks are underway. Satellite phones may provide an especially prominent option. Those phones are widely deployed both by BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies. General William Shelton (USAF-Ret.) who directed the U.S. Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these

---

<sup>150</sup> Russ Banham, "DDoS Attacks Evolve To Conscript Devices Onto The IoT," *Forbes*, February 4, 2018, <https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#4b5a43a86aaa>.

<sup>151</sup> "About Alerts," *NERC*, n.d.a., <http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx>.

<sup>152</sup> *Ibid.*

counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community.”<sup>153</sup>

The most difficult challenges for communications in a GSE would emerge as BPS entities implement emergency orders, and power companies coordinate with DOE on emergency operations and respond to follow-on strikes. Communications systems are likely to be under comprehensive attack during this stage. To prepare against that risk, power companies are ramping up their investments in emergency communications systems that are hardened against cyber and physical attacks, and can be used to sustain critical grid functions even if satellite phones fail.<sup>154</sup> Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are underway in building dark fiber or other survivable links between BPS entities – much less between those entities and DOE. The National Infrastructure Advisory Council study on *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish “separate, secure communications networks specifically designated for the most critical cyber networks, including ‘dark fiber’ networks for critical control system traffic and reserved spectrum for backup communications during emergencies.”<sup>155</sup>

The study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities “can communicate with utility crews working in the field to manually restore power” and conduct other post-attack operations.<sup>156</sup> Survivable communications systems will also need to enable the same multi-company decision-making and coordination with government that the ESCC already employs for hurricanes and other natural disasters. The development and deployment of such systems must be part of broader effort to prepare for grid security emergencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when they are needed most.

### **3. Securing Sensitive Emergency Orders and Classified Information**

Certain types of emergency orders may be vulnerable to countermeasures if adversaries gain access to them. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as

---

<sup>153</sup> General William L. Shelton, USAF (Ret), “Threats to Space Assets and Implications for Homeland Security,” *Written Testimony Before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*, March 29, 2017, p. 3, <http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf>.

<sup>154</sup> Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC), *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans – Further Joint Study: Planning Restoration Absent SCADA or EMS (PRASE)*, June 2017, p. 15.

<sup>155</sup> NIAC, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, August 2017, p. 7. <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>

<sup>156</sup> *Ibid.*



possible, lest those operations create incentives for adversaries to strike before their APTs were disabled. When attacks are underway, it could be useful to deny adversaries the knowledge of where and how BPS entities were prioritizing the flow of power to key military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The Federal Power Act and subsequent GSE Rule provide for the sharing of classified information in grid security emergencies. The GSE Rule specifies that:

To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.<sup>157</sup>

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program (CRISP) already have mechanisms and protocols for sharing and securing classified threat data with BPS entities cleared for access to that data.<sup>158</sup> Industry and government partners should consider building on those mechanisms to support the issuance of classified EOs. However, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Moreover, for utilities with cleared personnel on their staffs, an even smaller number possess the Sensitive Compartmented Information Facilities (SCIFs) or other infrastructure and government approvals to store classified information. To address those limitations, the GSE Rule clarifies that the Secretary may declassify information critical to the emergency response.<sup>159</sup> But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of Combatant Commander operational plans; when EOs may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

#### **4. Communicating with the American People**

Adversaries may attack the grid not only to disrupt national defense and the economy, but also to gain political leverage over U.S. leaders by inciting public panic and disorder. A presidential declaration that the grid faced imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks

---

<sup>157</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1182.

<sup>158</sup> “Energy Sector Cybersecurity Preparedness,” *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

<sup>159</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1778.

and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the U.S. public.

Pre-planning for public messaging to accompany GSE declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Providing for unity of messaging with governors and other elected officials on estimated times of restoration (ETRs) can present significant challenges in such events. However, those difficulties will be dwarfed by the problems that cyberattacks will create. GridEx IV (November 2017) highlighted a number of such problems. They include:

- Adversary use of information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety;
- Disruption of normal means of communication on which the public will rely for information about the event; and
- Inherent difficulties of estimating ETRs when adversaries employ advanced persistent threats that enable repeated re-attacks and disruptions in grid service until eradicated from BPS networks.

The ESCC and its members are developing playbooks to help meet these challenges, and to support public messaging in the event of cyber or physical attacks against the grid.<sup>160</sup> Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that Presidential GSE declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Pre-planning for message coordination with Canada and Mexico could also be helpful and might leverage the Federal Power Act's provisions for such multi-national consultations concerning the issuance of emergency orders.<sup>161</sup>

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. Some orders that will be valuable for protecting grid reliability, including EOs for prioritized load shedding, could cut off electricity to many thousands of customers in order to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by pre-planned communications playbooks to address customer concerns.

### **C. THE DEEPER VALUE PROPOSITION FOR EMERGENCY ORDERS: ENFORCEMENT, WAIVERS, AND COST RECOVERY**

---

<sup>160</sup> "ESCC," *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.

<sup>161</sup> 16 U.S.C. § 824o-1, Section (b)(3), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

Conservative operations offer an attractive starting point to develop pre-attack emergency orders because so many power companies already have extensive, frequently-used COs in place. For post-attack orders, NERC reliability standards provide a similarly well-established foundation for load shedding and other extraordinary measures. Emergency orders to accelerate power restoration can draw on a mutual assistance system that utilities have been refining for decades. These existing means of protecting and restoring grid reliability are so effective that they beg the question: how can emergency orders add value for defending the bulk power system and provide benefits beyond those that industry-based measures already offer?

EOs provide a unique means to ensure that BPS entities' emergency plans directly support U.S. deterrence goals and other national security priorities. As DOE and its partners identify critical electric infrastructure and defense critical electric infrastructure, and share that data with BPS entities, the electric industry will also be better positioned to develop utility-specific plans to sustain or restore service to vital facilities.

The development of template emergency orders will provide other benefits as well. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting COs to meet the specialized challenges posed by cyber and physical threats.<sup>162</sup> The industry-government process to develop emergency orders will provide a basis to share emerging best practices and embed them in utility plans for grid security emergencies.

The EO development process will also help protect grid reliability against nationwide threats. While hurricanes and other familiar natural hazards affect only limited geographic areas, adversaries may use cyber weapons to simultaneously attack all three interconnections in the United States. Communicating EOs in real time to utilities across the country may pose a challenge. DOE and the electricity subsector already have mechanisms in place to alert utilities when adversaries are implanting malware on critical systems, including the Cybersecurity Risk Information Sharing Program (CRISP) and other E-ISAC notification procedures and portals.<sup>163</sup> This includes the E-ISAC's new "Critical Broadcast Program," which is intended to operationalize their information sharing capabilities.<sup>164</sup> The Federal Bureau of Investigation (FBI) and DHS also issue alerts to the energy sector, as in the case of Nuclear 17 (June 2017)

---

<sup>162</sup> See, for example, PJM, *PJM Manual 13: Emergency Operations* Revision 64, June 1, 2017, p. 73; Todd Lucas (Southern Company), "Conservative Operations," (presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, Colorado, September 18-19, 2013), <http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf>; and SERC Reliability Corporation, *Conservative Operations Guidelines* Guide-800-101, May 20, 2015, [https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines\\_rev-0-\(05-20-15\).pdf?sfvrsn=2](https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2).

<sup>163</sup> "Energy Sector Cybersecurity Preparedness," *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>; "Electricity ISAC," *NERC*, n.d.a., <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>164</sup> The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See: Bill Lawrence, Charlotte de Seibert, and Philip Daigle, "E-ISAC Update," (presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, Florida, March 6-7, 2018), <https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf>.

and Crash Override.<sup>165</sup> However, when the President determines that there is an imminent danger of attacks on the grid, the Secretary will need a speedy and reliable system to trigger the implementation of conservative operations (including, potentially, specialized malware search and eradication measures) on a nationwide basis. Leveraging existing alert systems to support the issuance and execution of EOs will expedite preparedness for GSEs. It will also be essential to assess how adversaries might seek to disrupt the use of these existing systems, and supplement them as needed.

Developing EOs will facilitate nationwide exercises as well. NERC already requires BPS entities to exercise their individual emergency plans. In the GridEx exercise series, over 100 utilities across the United States and Canada exercise their plans against combined cyber-physical attacks and have an opportunity to share lessons learned. Building template emergency orders and utility-specific implementation plans would provide an even stronger basis for coordinated, multi-entity exercises against a notional threat, including the issuance and execution of emergency orders for all three phases of grid security emergencies.

Beyond these preparedness benefits, specific components of the Federal Power Act and GSE Rule create additional opportunities for added value – particularly if industry and government partners plan in advance for their mutual benefit.

## **1. Enforcement and Political “Top Cover”**

The GSE Rule specifies that “in accordance with available enforcement authorities, the Secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that order.”<sup>166</sup> The prospect that BPS entities will be punished for refusing to comply with poorly-conceived orders could raise concerns over the possible misuse of the Secretary’s enforcement powers. To help address those concerns, the Rule lays out a process by which entities can request clarification or reconsideration of orders issued to them.<sup>167</sup> How that process would actually function in the midst of nationwide attacks on the grid is uncertain.

However, pre-event coordination between industry and government could turn the looming threat of mandatory EO compliance into a mutually-beneficial arrangement. Rather than rely solely on adjudication mechanisms after the Secretary issues orders, DOE should collaborate with utilities to develop and refine orders in ways consistent with existing utility emergency procedures and

---

<sup>165</sup> The initial July alert was sent directly to energy sector stakeholders. See: Ellen Nakashima, “U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks,” *Washington Post*, July 8, 2017, [https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47\\_story.html?utm\\_term=.6ba8bdc7d36f](https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?utm_term=.6ba8bdc7d36f). FBI and DHS later released a public alert in October 2017. See: “Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Readiness Team*, October 20, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-293A>. For the CrashOverride alert, see: “Alert (TA17-163A) CrashOverride Malware,” *United States Computer Emergency Readiness Team*, June 12, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-163A>.

<sup>166</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1182.

<sup>167</sup> *Ibid.*, at pp. 1181-1182.

operational constraints. Doing so would – ideally – transform the mandatory nature of EOs into an advantage for utilities rather than a potential problem by leveraging the benefits that EOs provide for actions that these utilities would ordinarily carry out to protect or restore their systems. As examined in the two following sub-sections, those benefits include indemnification from environmental and other regulatory requirements, and the potential to recover costs incurred while carrying out the orders. With proper consultation, mandatory EOs could therefore serve to protect and compensate utilities for the very emergency actions required to protect their own systems.

The mandatory nature of EOs would also strengthen industry-wide security measures. NERC-developed (and FERC-approved) mandatory reliability standards and requirements to protect critical infrastructure from cyber and physical threats already help protect grid reliability against attacks by providing for consistent, nationwide adherence to those standards and the planning, training, and exercising requirements they entail. Some utilities voluntarily take further measures necessary to protect their systems from cyber threats. However, due to the interconnected nature of the BPS, the grid is only as strong as its weakest links.<sup>168</sup> The disparity in BPS entities' hardening efforts against adversarial threats means that even those that exceed NERC standard requirements remain potentially vulnerable. Creating mandatory emergency orders could help bridge the gap in protection against grid security emergencies, especially if BPS entities help shape those orders to go above and beyond the benefits of existing mandatory provisions for reliability.

Response operations provide an immediate opportunity to achieve such “value added” in designing EOs. The Electricity Subsector Coordinating Council serves as the principal liaison between the Federal government and the electric industry in responding to severe power outages. The Council includes entities of all ownership structures in the subsector, including investor-owned utilities, electric cooperatives, municipally-owned utilities, and federal utilities. This industry-wide representation enables the ESCC to serve as the “center of gravity” for coordinating response operations with DOE and other government partners. Moreover, after decades of use in hurricanes and other severe natural hazards, the Council's collaborative mechanisms offer a strong, industry-developed and time-tested basis for responding to grid security emergencies.

The ESCC is already adapting its response coordination mechanisms to support restoration against manmade threats – most notably by establishing a Cyber Mutual Assistance program.<sup>169</sup> Moreover, following Superstorm Sandy, investor-owned utilities (led by the Edison Electric Institute) also established new mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States under the National Response Event

---

<sup>168</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation's Electricity System: Second Installment of the QER*, January 2017, p. 1-33.

<sup>169</sup> Electricity Subsector Coordinating Council, *The ESCC's Cyber Mutual Assistance Program*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.2>.



(NRE) framework.<sup>170</sup> Both initiatives will be vital for responding to grid security emergencies that entail multi-region disruptions of the BPS.

The representative structure of the ESCC provides additional advantages for preparedness against GSEs. While only a limited number of industry CEOs service on the Council at any one time, those CEOs are able to reach out to other grid owners and operators across the United States and help coordinate the provision of restoration personnel and equipment on a nationwide basis. These CEOs can also request additional resources and strategic guidance when available response assets are stretched thin. However, all such assistance is voluntary; the ESCC lacks the authority to require utilities to provide assistance or to prioritize restoration operations when available resources cannot meet all requests for aid.

Emergency orders could offer DOE an additional means to support industry response operations and ensure that they account for government priorities. The Department's support could be especially valuable against cyberattacks. When hurricanes strike the Gulf Coast or the Southeast, for example, utilities on the West Coast can contribute response crews, bucket trucks, and other response assets, safe in the knowledge that the storm will not affect their own service areas. Cyberattacks will create a very different environment for providing voluntary assistance. Attacks on one utility may presage an attack on all. Utility CEOs who donate scarce cyber response personnel and assets to support another company will be at risk of suffering similar attacks, and – potentially – of suffering more severe blackouts because those personnel were already committed elsewhere.<sup>171</sup> The Cyber Mutual Assistance (CMA) Program is developing specialized protocols to deal with these challenges. However, as the ESCC notes, “participation in the CMA Program, as well as any decision to respond to requests for assistance made under the CMA Program, is voluntary.”<sup>172</sup> While the emergency order process will need to take into account the risk of re-attack in cyber incidents, EOs could nevertheless mandate compliance with industry-government decisions on restoration priorities, and reinforce the subsector's voluntary system for providing assistance in National Level Events.

Utilities may also find it helpful that their actions to meet broader national priorities, which are likely to provoke intense opposition from state and local government leaders, state Public Utility Commissioners, and customers, will be Federally-mandated. In Superstorm Sandy and other severe weather events, governors have sometimes been reluctant to support the flow of power restoration crews and equipment to neighboring states until all of their own citizens (read: voters) had their lights back on. Cyber and physical attacks on the grid could create still stronger political disincentives to share restoration assets, especially if adversaries use information warfare to inflame citizen fears over potential outages and threats to public safety. Such attacks could also put utility CEOs in the unenviable position of having to manage shortfalls in available

---

<sup>170</sup> Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, October 2016,

[http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA\\_101FINAL.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf).

<sup>171</sup> North American Electric Reliability Corporation, *Cyber Attack Task Force: Final Report*, March 2012, p. 29, [http://www.nerc.com/%20docs/cip/catf/12-CATF\\_Final\\_Report\\_BOT\\_clean\\_Mar\\_26\\_2012-Board%20Accepted%200521.pdf](http://www.nerc.com/%20docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf).

<sup>172</sup> Electricity Subsector Coordinating Council, *The ESCC's Cyber Mutual Assistance Program*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.2>.

power by depriving lower priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The Secretary of Energy can give CEOs political top cover for taking such unpopular actions, rather than leave utility leaders to act on a voluntary basis and bear the full brunt of explaining why they did so – or have them not serve national priorities at all.

## **2. Environmental, Regulatory, and Legal Waivers**

In amending the Federal Power Act to address grid security emergencies, Congress also provided power companies with an important protection for complying with emergency orders – one which they might not receive by implementing conservative operations or other emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate grid reliability standards approved by the Federal Energy Regulatory Commission (FERC) or other rules or provisions under FPA, the Act specifies that those actions “shall not be considered a violation” of those provisions. Such waivers of enforcement apply unless a complying entity acts in a “grossly negligent manner.”<sup>173</sup>

The FAST Act amendments to the FPA also introduced broader protections into section 202(c) which absolve entities from violations of Federal, state or local environment law or regulation that occur as a result of complying with an order. That provision also shields complying entities from “any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation.”<sup>174</sup> These protections also apply to Section 215A emergency orders.<sup>175</sup>

These waivers will be especially valuable for certain types of emergency orders. For example, if the Secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service could also violate FERC-approved reliability standards. Separating pre-planned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards.

The waiver process under the FPA is structured to function smoothly and automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that, in the course of complying with an emergency order, a BPS entity has acted in “a grossly negligent manner.” Nevertheless, specifying the waiver protections provided by a given EO, specific to what the Secretary is ordering entities to do, could benefit the collective response to grid security emergencies. In particular, identifying the protections provided by the EO would give complying entities assurances of their protection, and limit potential disputes with regulatory bodies.

Moreover, for certain types of emergency orders, pre-planning for regulatory waivers could comprise a necessary component of the order development process. For example, the amended

---

<sup>173</sup> 16 U.S.C. § 824o–1, Section (f)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>174</sup> 16 U.S.C. § 824a, Section (c)(3), <https://www.law.cornell.edu/uscode/text/16/824a>.

<sup>175</sup> 16 U.S.C. § 824o–1, Section (f)(2), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

FPA does not provide waivers for Nuclear Regulatory Commission (NRC) regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the NRC would enforce a violation of their regulations by a nuclear generation entity complying with an EO. The worst time to adjudicate such a dispute, however, would be in the midst of a GSE. DOE should therefore engage with the NRC to examine waiver options (or, potentially, options to exclude nuclear generators from EO requirements) as the EO development process goes forward.

Pre-planning will also be vital for EOs that accelerate power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that “the storage of strategically located spare large power transformers” and other critical grid components “will reduce the vulnerability of the United States to multiple risks facing electric grid reliability,” including cyber and physical attacks.<sup>176</sup> Accordingly, Congress required DOE to develop a Strategic Transformer Reserve Plan to determine the number and type of spare Large Power Transformers (LPTs) that should be stored, and examine issues associated with transporting those spares.<sup>177</sup>

DOE responded by providing a Strategic Transformer Reserve (March 2017) report. The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a larger pool of spare LPTs than DOE had anticipated and that a Federally-owned reserve is not needed.<sup>178</sup> However, the Plan also found that it was also crucial to ensure that LPTs can be efficiently moved during national emergencies.<sup>179</sup>

Emergency orders can play a critical role in facilitating that movement. The higher voltage classes of LPTs, including 765 kilovolt (KV) transformers, are as big as a house and can only be moved – slowly and very carefully – by specialized heavy-haul trucks, rail cars, and barges. Under the auspices of the ESCC, utilities have established a Transformer Transportation Working Group to analyze the problems posed by the emergency movement of LPTs and build collaborative plans with transportation companies and associations. A key finding of the Group’s analysis: regulatory waivers will be critical to expedite LPT movement, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.<sup>180</sup>

---

<sup>176</sup> “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1779, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>177</sup> *Ibid.*, at pp. 1780-1782.

<sup>178</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 21, <https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>179</sup> “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1781, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>180</sup> ICF (for the Department of Energy), *Assessment of Large Power Transformer Risk Mitigation Strategies*, October 2016, pp. 22-23, <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf>.

DOE's 2017 transformer report committed the Department to coordinating with the Transformer Transportation Working Group (TTWG) "to improve and optimize transportation planning in response to a significant national event impacting the electricity grid."<sup>181</sup> However, the report did not examine how emergency orders and implementation plans might speed LPT transportation. As DOE collaborates with the TTWG and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols not addressed by the FPA that pose the greatest impediments to LPT movement, and pre-plan to waive them if the President declares a GSE.

Those coordination efforts will face an immediate challenge: the Secretary of Energy lacks the statutory authority to waive key transportation regulations. Most Federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of the U.S. Department of Transportation (DOT). Federal regulations and emergency operations that would govern barge movement of transformers, which could be critical for restoring power for coastal cities and along the Mississippi-Ohio river system of inland waterways, are overseen by the U.S. Coast Guard (USCG) and the U.S. Army Corps of Engineers (USACE). State and local transportation regulations and permitting requirements will also pose major impediments to emergency LPT road movement unless adequate waivers are in place to lift them.

The EO development process should therefore include coordination with non-DOE regulatory authorities. The Department of Energy has extensive experience in collaborating with other Federal, state, local, tribal and territorial (SLTT) agencies. That experience has been especially valuable for building plans and improving coordination for restoration operations under the auspices of Emergency Response Function #12 – Energy. Moreover, as individual utilities have created contingency plans for emergency transportation with road, rail, and barge companies, they have also built relationships with SLTT agencies and government leaders. Utilities and DOE should build on those relationships and plans to launch a systematic, integrated effort to provide for regulatory waivers where (under the FPA) enforcement of violations would not automatically be waived.

Over the longer term, industry and government partners should also consider whether complying entities should have protections beyond those currently in the Federal Power Act. Prioritized load shedding for extended periods will create "winners and losers" in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other Section 9+ assets may leave dialysis centers, small urgent care centers, and facilities for special needs citizens with shortfalls in electric service. Cutting off power to lower priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.<sup>182</sup>

---

<sup>181</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 22, <https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>182</sup> Alison Frankel, "Can customers sue power companies for outages? Yes, but it's hard to win," *Reuters*, November 9, 2012, <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>.

If these risks of exposure are sufficiently severe, Congress should consider providing additional protections for BPS entities that are complying with emergency orders.

### **3. Cost Recovery for Emergency Operations and Supporting Investments in Grid Infrastructure**

Complying with emergency orders may force utilities to incur costs above and beyond their normal operating expenses. The Federal Power Act states that if FERC determines “that owners, operators, or users of critical electric infrastructure have incurred substantial costs” in complying with an EO, FERC shall “establish a mechanism that permits such owners, operators, or users to recover such costs.”<sup>183</sup> Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other EOs could require reimbursement through FERC-directed mechanisms as well.

The Act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that EOs require owners or operators of DCEI to take emergency measures, the owners or operators of critical defense facilities that rely on such infrastructure “shall bear the full incremental costs of those measures.”<sup>184</sup> Fair warning to the Department of Defense: DOD should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- Attacks create major blackouts and deprive utilities of revenue;
- Emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- Adversaries disrupt financial markets, either through direct cyberattacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.<sup>185</sup>

Power companies are rapidly strengthening their plans and capabilities for cross-sector support with the financial services sector (and with the communications sector on which they depend).<sup>186</sup> These efforts should include the development of contingency plans for financial services

---

<sup>183</sup> The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs “prudently,” and that those costs “cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users. 16 U.S.C. § 824o–1, Section (b)(6)(A), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

<sup>184</sup> 16 U.S.C. § 824o–1, Section (b)(6)(B), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

<sup>185</sup> North American Electric Reliability Corporation, *Grid Security Exercise: GridEx III Report*, March 2016, p. 15, <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.

<sup>186</sup> See, for example, the Strategic Infrastructure Coordinating Council (SICC). Electricity Subsector Coordinating Council, *ESCC Initiatives*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf>.



companies (in coordination with the Department of Treasury and DOE) to help utilities meet the time-urgent expenses of responding to grid security emergencies.

In addition, to facilitate the EO reimbursement process provided for in the Federal Power Act, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with EOs will be more difficult once attacks are underway. That is especially true since the text of the FPA leaves substantial ambiguities to resolve – starting with the definition of who are “users” of critical electric infrastructure and therefore potentially eligible for reimbursement.

Such users might well include electricity distribution companies who are not BPS entities (and are therefore not subject to emergency orders), but who could be vital to protect and restore the flow of power between high voltage transmission systems and regional hospitals and other critical facilities. For example, intentional load shedding operations to stabilize the grid are nearly all performed at the distribution level, and distribution providers would also be performing the switching for required to implement rotating blackouts. For the many BPS entities that are not vertically integrated and do not own and operate “local” distribution utilities excluded from the FPA’s BPS definition, it will be essential to include those local distribution providers in contingency plans to execute emergency orders. Given the costs that distribution systems may incur in implementing EOs, FERC and its partners should clarify eligibility for reimbursement and the process by which grid operators will recover their costs as soon as possible.

Cost recovery for investments in grid infrastructure to facilitate emergency orders will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. However, other EOs may be impossible to execute unless BPS entities make additional investments in infrastructure. For vital but remote military bases that are served by a single transmission line, it will be near-useless to order transmission operators to protect or rapidly restore service to those bases if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure they can help defeat U.S. adversaries when the Nation is under attack. DOD will need to ensure it has a cost recovery mechanism to reimburse DCEI owners for making such investments.

For pre-planned power islands to be even remotely viable as an EO design option, many such islands will also require at least some infrastructure construction. Ideally, these pre-planned islands will make use of existing generation, transmission, and distribution assets within their service footprints so that they can separate from the grid and still be able to provide reliable electric service to the Section 9+ assets insider their borders. But many areas that might be designed to function as islands in a GSE will lack adequate infrastructure to do so. The interconnected design of the grid enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Pre-planned power islands will not only lose those reliability benefits, but also have to make do with infrastructure that

utilities built and aligned to be supporting components of the interconnected grid – *not* self-sustaining islands that would be stood up in grid security emergencies. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: many EOs could require spending on new transmission lines and other grid infrastructure in order to be effectively implemented.

The provisions of the FPA pertaining to emergency orders do not explicitly authorize reimbursement for such infrastructure investments. While the Act requires FERC to establish a mechanism to enable owners, users, and operators of CEI and DCEI to recover their costs of complying with emergency orders, those funding provisions do not mention pre-attack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover their costs for infrastructure investments against cyber and physical attacks.<sup>187</sup> FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate EO execution.

Similar discussions will be valuable with state public utility commissions (PUCs). As noted above, distribution systems will likely need to play a vital role in implementing emergency orders. PUCs have primary regulatory authority over distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. Public utility commissions could also make important contributions to reviewing proposed EO implementation plans that would be executed within their respective states, particularly for orders that distribution systems would need to help implement.

The Federal Power Act opens the door to discussions with PUCs over investments and planning to support EO execution. The Act states that FERC and the Secretary of Energy “shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions.”<sup>188</sup> Initiating such discussions with the National Association of Regulated Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has conducted detailed analysis of criteria for assessing the prudence of investments against cyber and physical attacks, and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

---

<sup>187</sup> See, for example: Federal Energy Regulatory Commission (FERC), *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies*, Statement of Policy (96 FERC ¶ 61,299), September 14, 2011; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), April 19, 2004, pp. 10-11 (2004); FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), September 22, 2016, p. 60.

<sup>188</sup> 16 U.S.C. § 824o–1, Section (d)(4), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

## **V. CONCLUSIONS AND RECOMMENDATIONS FOR FOLLOW-ON ANALYSIS**

[To be completed by April 30, 2018]

From: [Cheryl LaFleur](#)  
To: [David Ortiz](#); [Joseph McClelland](#)  
Cc: [Kris Fitzpatrick](#); [Jessica Cockrell](#)  
Subject: Fwd: Draft Study on Grid Security Emergencies  
Date: Thursday, April 26, 2018 6:24:09 PM  
Attachments: [APL GSE Study Sections I-IV April 26 2018.docx](#)  
[ATT00001.htm](#)

---

David and Joe if (and only if) you have anyone w the time to read this paper from Paul Stockton I'd appreciate it. Unrealistic timeline but important topic. I will try to take a look also. Thank you.

Sent from my iPad

Begin forwarded message:

**From:** Paul Stockton <[pstockton@sonecon.com](mailto:pstockton@sonecon.com)>  
**Date:** April 26, 2018 at 4:20:08 PM EDT  
**To:** Cheryl LaFleur <[Cheryl.LaFleur@ferc.gov](mailto:Cheryl.LaFleur@ferc.gov)>  
**Subject:** Draft Study on Grid Security Emergencies

Cheryl, thanks again for meeting me for lunch, and all of the insights you have shared with me on grid resilience against emerging cyber and physical threats. Attached is the draft study I mentioned on grid security emergencies/FPA emergency orders.. I'd very much appreciate it if you could give the study the old wire brush treatment! The publisher, Johns Hopkins University's Applied Physics Laboratory, wants the final version by May 2, 2018. Please feel free to share with your staff.

Best, Paul

**Paul Stockton**  
**Managing Director, Sonecon, LLC**  
**325 7<sup>th</sup> Street NW**  
**Suite 250**  
**Washington, D.C. 20004**  
**202-393-2228**  
**Cell: 703 945 6574**  
[pstockton@sonecon.com](mailto:pstockton@sonecon.com)

*DRAFT: NOT FOR USE OR CITATION  
WITHOUT PERMISSION OF THE AUTHOR*

# **RESILIENCE FOR GRID SECURITY EMERGENCIES: OPPORTUNITIES FOR INDUSTRY-GOVERNMENT COLLABORATION**

Paul N. Stockton (pstockton@sonecon.com)  
Report for the Johns Hopkins University Applied Physics Laboratory (APL)  
April 26, 2018

## **EXECUTIVE SUMMARY**

The United States Congress has opened the door to novel strategies for defending the U.S. electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act in December 2015, Congress granted the Secretary of Energy vast new authorities to use when the President declares that a grid security emergency exists. Most important, legislators authorized the Secretary of Energy to issue emergency orders to grid owners and operators to protect and restore grid reliability when attacks on their systems are imminent or underway.<sup>1</sup> The Federal Power Act is silent, however, on what the Secretary might order these owners and operators to do and how emergency orders can effectively bolster their protection efforts.

The onslaught of an attack would be the worst possible time to develop such orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid which could then be adjusted to fit the specific circumstances of an attack. Developing such orders in advance would help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. In turn, those contingency plans could provide the basis for training and exercise initiatives to prepare for the attacks to come.

This study is structured help the electricity subsector partner with the Department of Energy (DOE) to develop emergency orders and meet the broader policy and operational challenges that grid security emergencies will entail. In particular, the study examines how these partners might develop emergency orders to protect grid reliability against potentially catastrophic cyber and physical attacks, and – if major blackouts occur – help utilities accelerate the restoration of power.

---

<sup>1</sup> The "Fixing America's Surface Transportation Act" [hereinafter referred to as the FAST Act], Public Law 114-94, *U.S. Statutes at Large* 129 (2015): pp. 1773-4, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.



DOE and their industry partners should develop emergency orders for three possible phases of grid security emergencies. The Federal Power Act specifies that the President can declare a grid security emergency (GSE) when there is “imminent danger” of an attack on electric infrastructure critical for national defense, economic security, and public health and safety. Strong foundations already exist for developing emergency orders for this initial, pre-attack phase of GSEs. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions, such as staffing up emergency operations centers, increasing available generation to help manage grid instabilities, and taking other precautionary measures.

Determining that a cyber or physical attack is imminent could be vastly more difficult than doing so for hurricanes. However, if the United States has sufficient warning of an attack, many of the same measures used to bolster preparedness against natural hazards might be adapted to provide pre-attack options for conservative operations. Promising opportunities also exist to develop measures tailored for cyber or physical threats. Emergency orders for conservative operations constitute “low hanging fruit;” industry and government partners should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The Federal Power Act also states that the President can declare a GSE when attacks are “occurring.” Industry and government partners should develop a second set of orders to use once attacks are underway, both to prevent power failures from cascading across the United States and to sustain electric service to major regional hospitals and other critical facilities. Existing electric industry plans and capabilities provide a strong basis to develop such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Emergency orders for equivalent *extraordinary measures* could provide useful “arrows in the quiver” in grid security emergencies, and could help integrate national security priorities into existing utility plans to counter grid instabilities.

A third set of potential emergency orders would help utilities accelerate power restoration if blackouts occur. Attacks that damage or destroy large number of high voltage transformers or other difficult-to-replace equipment could create outages that darken major portions of the United States for many weeks or even months. Power companies and DOE already have initiatives underway to meet this challenge. They should also collaborate to develop emergency orders to *accelerate restoration*. In particular, orders might be drafted to account for the risk that adversaries will continue attacking after their initial salvo, and launch follow-on strikes to disrupt restoration operations and lengthen U.S. power outages.

Of course, Russia, China, and other potential adversaries will not strike the grid merely to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to U.S. Defense installations, ports, and other civilian infrastructure essential for deploying and sustaining forces to the region. Emergency orders can be designed to help deter – and, if necessary, defeat – such attacks. This study proposes specific

options to do so, in support of the *National Security Strategy of the United States of America* and other sources of U.S. policy guidance.

The study also identifies ways that government and industry can pre-plan to communicate with the American people if adversaries strike. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks – and, potentially, attack the phone and internet-based communications systems on which utilities typically use coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications “playbooks” to prepare for grid security emergencies, and make doing so a core component of the emergency order development process.

These partners should also pre-plan to take advantage of an especially valuable way in which Congress amended the Federal Power Act: the creation of new provisions for emergency regulatory waivers and cost recovery for power companies. Legislators recognized that to comply with emergency orders, grid owners and operators might have to violate environmental regulations and other standards. The Act now protects entities from the enforcement of such violations if they occur as the result of complying with emergency orders. The FPA also provides for the recovery of costs that companies will incur in implementing those orders. This study suggests additional measures that industry and government may want to consider to facilitate compliance and reinforce the “value added” of emergency orders for countering attacks on the grid.

In addition, government and industry partners should examine the triggers and thresholds for declaring grid security emergencies and issuing emergency orders. Major ambiguities surround the criteria for making such declarations, especially for attacks that may be imminent. One option to clarify these criteria would be to leverage the electric industry’s focus on preserving “adequate levels of reliability,” and declare emergencies when adversaries are poised to create cascading power failures and other major disruptions across multiple states. However, the President should also retain the flexibility to declare GSEs for a broad range of other contingencies.

Industry and government partners should also identify opportunities to build broader resilience for grid security emergencies. Intensive follow-on work will be required to finalize the development of emergency orders and build utility-specific contingency plans to implement them in ways that account for accelerating structural changes in the electricity subsector (including the large-scale integration of wind and solar generation). Those collaborative efforts will require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, three additional opportunities for progress could offer special benefits for strengthening GSE preparedness. First, DOE and its industry partners should consider expanding the scope of EO planning across the energy sector to address the risk that adversaries will attack

both the grid and the natural gas transmission system on which power generation increasingly depends. Second, these partners should develop additional options to counter the risk that adversaries will conduct targeted information operations to sow disorder and magnify the disruptive effects of attacks on the grid. Third, government leaders should also explore strategic opportunities to capitalize on the improvements in grid resilience that EOs and related preparedness initiatives will make possible. In particular, these leaders should consider developing integrated offense-defense operational plans to strengthen the deterrence of cyberattacks against the United States, and to help manage the escalation (and speed the favorable resolution) of conflicts that do occur.

## **I. DEVELOPING EMERGENCY ORDERS UNDER THE FEDERAL POWER ACT: OVERARCHING GOALS AND DESIGN REQUIREMENTS**

The foundational importance of the electric grid makes it a prime target for attack. As Secretary of Energy Richard Perry emphasizes, “America’s greatness depends on a reliable, resilient electric grid” that can power the economy, support national defense, and provide for the necessities of modern life.<sup>2</sup> To prevent adversaries from exploiting this extraordinary dependence on the U.S. electric system, the Department of Energy and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter – and, if necessary, defeat – attacks on the grid.<sup>3</sup>

The text of the FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the “FAST Act” amendments to the FPA, legislators greatly expanded the Secretary of Energy’s authority to issue emergency orders to grid owners and operators. Under Section 215A of the Act, “the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgement of the Secretary to protect or restore the reliability” of the critical grid infrastructure in a grid security emergency.<sup>4</sup>

---

<sup>2</sup> Secretary of Energy Richard Perry, *Letter to the Federal Energy Regulatory Commission Re: Secretary of Energy’s Direction that the Federal Energy Regulatory Commission Issue Grid Resiliency Rules Pursuant to the Secretary’s Authority Under Section 403 of the Department of Energy Organization Act*, September 28, 2017, <https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf>.

<sup>3</sup> As noted above, the 2015 FAST Act amendments to the Federal Power Act (FPA) provide the authority to do so. Prior to 2015, Section 202(c) of the FPA already authorized the Secretary of Energy to issue emergency orders to order “temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest.” That provision also specified that the Secretary could exercise such powers “during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes.” See: “DOE’s Use of Federal Power Act Emergency Authority,” *Department of Energy*, 2017, <https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use>. The 2015 FAST Act amendments to the FPA gave the Secretary further powers (mostly incorporated in Section 215A of the Act), which are the primary focus of this study.

<sup>4</sup> Before the Secretary can issue emergency orders, the President must first declare a grid security emergency (GSE). The analysis that follows examines the definition of GSEs in the FPA. This analysis also examines the focus of

However, legislators provided only limited guidance on what the Secretary might order power companies to do. The Department of Energy and their partners in the electricity subsector have begun to assess which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats.

This portion of the study (Section I) examines the near and longer-term advantages of developing emergency orders before adversaries strike. Section I also identifies specific industry and government partners who might participate in this development process, and highlights the overall design requirements that emergency orders may need to meet, both to comply with the Federal Power Act and to address the broader challenges that grid security emergencies will pose.

The Act specifies that before the Secretary can issue emergency orders, the President must first declare a grid security emergency (GSE). Section II surveys the types of threats that can trigger a GSE and explains why this study focuses on the risk of cyber and physical attacks. Section II also examines possible thresholds and decision criteria that the President might use to determine whether a GSE exists, and how consultations and information sharing with power companies might support such determinations.

Section III provides a framework for developing emergency orders for use in three phases of GSEs: when the President determines that there is an imminent danger of attacks, when attacks are underway, and when electric companies are restoring power – potentially in the face of continuing attacks on the grid. Section III also provides examples of emergency orders (EOs) and identifies promising options for further analysis.

Section IV analyzes the broader design challenges that emergency orders may entail. These include: 1) tailoring EOs to help deter attacks on the United States, and help the U.S. military defeat adversaries if deterrence fails; 2) ensuring that the Secretary can effectively communicate emergency orders to power companies if phone and internet communications are disrupted, and pre-planning to communicate with the American people when attacks are underway; and 3) strengthening the “value added” of emergency orders for the electric industry by providing political top cover for unpopular emergency measures, as well as regulatory waivers and cost recovery beyond the provisions in the FPA. Section V identifies issues for further analysis that may offer special benefits for building preparedness for grid security emergencies.

## **A. IMPERATIVES FOR GOVERNMENT-INDUSTRY COLLABORATION**

The Secretary’s new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, “the nine most terrifying words in the English language are

---

emergency orders on protecting or restoring the reliability of critical electric infrastructure and defense critical electric infrastructure in the bulk power system (BPS), and the definition of these terms in the Act.

‘I’m from the government and I’m here to help.’”<sup>5</sup> Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already beginning to manage such risks by incorporating industry recommendations on the process by which the Secretary should issue emergency orders (EOs), and – “if practicable” – consult with industry before those orders are issued.<sup>6</sup> The next collaborative step should be to include power companies in designing EOs. Grid owners and operators have unequalled knowledge of their own infrastructure and operating procedures, and have extensive experience in employing emergency measures to protect and restore grid resilience. They are well-positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses – and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders will assist them in protecting or restoring grid reliability, above and beyond the emergency measures that companies would already be taking on their own.

Industry will need government leadership as well. Federal guidance will be essential to ensure that emergency orders help achieve overarching U.S. security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing EOs to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.<sup>7</sup> Federal leadership will also be necessary to integrate criteria and decisions for issuing emergency orders into the broader U.S. incident response system established by Presidential Policy Directive 41: *United States Cyber Incident Coordination* (July 2016), the *National Response Framework* (June 2016), and other mechanisms and guidelines for coordinating response operations.<sup>8</sup> In addition, as provided for in the FPA and other sources of Federal guidance, government agencies (with industry support) will also need to identify the grid infrastructure that is most critical for protecting the U.S. economy, public health and safety, and the defense of the United States.<sup>9</sup>

Government participation will also be necessary to account for the support that DOE and other agencies may be able provide to industry in grid security emergencies. For example, if adversaries destroy large power transformers and other critical grid infrastructure, Federal, state,

---

<sup>5</sup> Ronald Reagan, “The President’s News Conference,” August 12, 1986, <http://www.presidency.ucsb.edu/ws/?pid=37733>.

<sup>6</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1176; EEI, “COMMENTS OF THE EDISON ELECTRIC INSTITUTE,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*, February 6, 2017; and IRC, “ISO-RTO Council Comments on Notice of Proposed Rulemaking,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*, February 6, 2017.

<sup>7</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017.

<sup>8</sup> White House, *Presidential Policy Directive - United States Cyber Incident Coordination*, July 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>; Department of Homeland Security, *National Response Framework: Third Edition*, June 2016.

<sup>9</sup> 16 U.S.C. § 824o-1, Section (c), <https://www.law.cornell.edu/uscode/text/16/824o-1>.



local, tribal, and territorial transportation agencies may be able to waive regulations and other requirements that would otherwise slow the movement of replacement transformers. The Department of Energy may not be able to order transportation agencies to issue such waivers. However, DOE can lead government-wide engagement to incorporate waiver planning and other support functions into emergency orders and provide a focal point for industry collaboration.<sup>10</sup> Most important of all: DOE is the Sector-Specific Agency for the energy sector and is uniquely positioned to partner with electric utilities in the EO development process.

## **1. Drafting Template Emergency Orders Before Attacks Occur**

The Federal Power Act specifies that before issuing emergency orders “the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action,” consult with appropriate power companies and other stakeholders in grid resilience.<sup>11</sup> In January 2018, the Department of Energy issued procedures for conducting such consultations and communicating emergency orders, and incorporated a number of recommendations proposed by power companies to strengthen industry-government coordination in grid security emergencies.<sup>12</sup>

But the need for action may be too urgent to permit such consultation before the Secretary issues emergency orders. Adversaries may launch cyberattacks on the grid with little or no warning. Indeed, they will have additional incentives to do so if they can preclude the effective use of emergency orders by minimizing opportunities for industry-government dialogue, and by disrupting communications between DOE and grid owners and operators.

To ensure that EOs will benefit from industry-government consultation, and to minimize the risk that DOE will have to design orders from scratch amidst the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, Assistant Secretary of Energy for Electricity Delivery and Energy Reliability, stated in March 2018 that “In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.”<sup>13</sup> Power companies and other

---

<sup>10</sup> The FAST Act amendments explicitly provide for such a role in cybersecurity planning and incident management. See: “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1779, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>11</sup> 16 U.S. Code § 824o-1, <https://www.law.cornell.edu/uscode/text/16/824o-1>. See also the notice of proposed rulemaking and request for comment: Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 81, No. 235 (2016), [https://energy.gov/sites/prod/files/2017/02/f34/DOE\\_FRDOC\\_0001-3281.pdf](https://energy.gov/sites/prod/files/2017/02/f34/DOE_FRDOC_0001-3281.pdf).

<sup>12</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1175.

<sup>13</sup> Bruce J. Walker, *Written Testimony Before the U.S. Senate Committee on Energy and Natural Resources*, March 1, 2018, [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=1C574731-A9C0-4E1C-9E05-15C492E332B1](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1)

electricity subsector organizations have also emphasized the need for industry and government to jointly develop orders before adversaries strike.<sup>14</sup>

Such collaborative efforts should initially focus on creating *template orders*: i.e., orders that lay out the basic types of actions that the Secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act’s potential value for the Secretary to issue general orders to “protect and restore the reliability of the grid.” Vague, overly broad directives cannot provide an adequate basis for utilities to build system-specific plans to implement them, or exercise and train utility personnel to do so. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for “maximum generation” and increased reserve margins to more aggressive, far-reaching measures.<sup>15</sup> The goals for such development efforts: 1) provide a menu of pre-agreed upon options from which the Secretary can choose as circumstances require, in consultation with industry (as provided for in the FPA); and 2) ensure that existing utility plans for prioritized power restoration and other emergency operations help achieve government-identified national security priorities.

In actual attacks, Russia, China, or other potential adversaries will employ country-specific malware and tactics, techniques, and procedures. Defense against those attacks will require equally tailored, threat-specific tactical and operational response measures. Over time, it may be possible to develop (and protect adversaries from stealing) emergency orders that account for these individualized defensive requirements. U.S. leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this study will examine the development of such integrated offense-defense plans as a future research priority.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military

---

<sup>14</sup> See: Joint Commenters, “COMMENTS OF AMERICAN PUBLIC POWER ASSOCIATION, LARGE PUBLIC POWER COUNCIL, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, AND TRANSMISSION ACCESS POLICY STUDY GROUP,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, February 23, 2017, <http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf>; NASEO, “COMMENTS OF THE NATIONAL ASSOCIATION OF STATE ENERGY OFFICIALS,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, n.d.a, [https://www.naseo.org/Data/Sites/1/naseo-comments\\_rin-1901-ab40.pdf](https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901-ab40.pdf); and EEI, “COMMENTS OF THE EDISON ELECTRIC INSTITUTE,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, February 6, 2017.

<sup>15</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help “maintain reliable operation while meeting ... unexpected outages of existing capacity.” See: NERC, “M-1 Reserve Margin,” 2017, <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.

bases, regional hospitals, and other critical facilities in their service area that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and present opportunities to improve order design and coordination. Training programs to prepare employees to carry out utility-specific plans to implement template orders should also get underway as soon as those orders are developed. On a larger scale, utilities will also be able to plan and exercise for the employment of template emergency orders under the Cyber Mutual Assistance (CMA) program. This program enables over a hundred utilities to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.<sup>16</sup> As the CMA program grows, it will provide increasingly valuable support for the nationwide execution of emergency orders.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the Secretary of Energy has the sole authority to issue EOs, the Secretary may request input from senior DOE staff on the benefits of specific options and the rationale for issuing those orders. The Secretary and DOE staffers may also need to brief the President and the National Security Council on proposed orders and the public messaging issues the orders entail. By developing EOs before GSEs occur and explaining how they will protect grid reliability, DOE and industry partners can strengthen the foundations for such deliberations and help design exercises for GSE decision making.

Over the longer term, industry and government leaders might structure their collaboration in order to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public-private and interagency coordination.<sup>17</sup> Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government-industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, the development of template emergency orders and contingency plans to implement them will require power companies to conduct extensive operational and engineering studies. The FAST Act amendments to the FPA provide no funding for such development efforts.

---

<sup>16</sup> “The ESCC’s Cyber Mutual Assistance Program,” *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1>.

<sup>17</sup> Richard Danzig, “Catastrophic Bioterrorism – What Is To Be Done?,” *Center for Technology and National Security Policy*, August 2003, [http://www.response-analytics.org/images/Danzig\\_Bioterror\\_Paper.pdf](http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf), pp. 5-7; Blue Ribbon Study Panel on Biodefense (Hudson Institute), *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts – Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*, October 2015, <http://www.biodefensestudy.org/a-national-blueprint-for-biodefense>, pp. 13 and 42-4.

Moreover, in order to build and effectively execute such plans, power companies will need to coordinate (and potentially share sensitive information) with a much wider array of partners as the development process goes forward.

## **2. The Bulk Power System as the Focus of GSE Declarations and Emergency Orders: Implications for EO Development**

Before examining these design requirements in further detail, an underlying constraint in the Federal Power Act merits analysis. The Act specifies that critical electric infrastructure includes only those assets that comprise the bulk power system (BPS). BPS assets are those “facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation facilities needed to maintain transmission system reliability.”<sup>18</sup> These bulk power system generation and transmission assets provide synchronized power across the three interconnections that serve the entire United States and parts of Mexico and Canada.<sup>19</sup>

However, as defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.<sup>20</sup> The FPA also specifies that emergency orders will apply to BPS owners and operators. That focus excludes local distribution providers, even if they provide the “last mile” of connectivity between transmission systems and military bases and other critical customers. The exclusion of local distribution providers has significant implications for the design and implementation of EOs, and poses political as well as technical challenges for protecting and restoring electric service.

The FPA states that the Secretary of Energy may issue emergency orders to a range of BPS “entities.”<sup>21</sup> These include:

***a. The Electric Reliability Organization.*** After blackouts cascaded across major portions of the United States in August 2003, Congress directed the Federal Energy Reliability Commission (FERC) to designate an Electric Reliability Organization (ERO) to enforce mandatory electric reliability rules on all users, owners, and operators of the U.S. bulk power system.<sup>22</sup> FERC appointed the North American Electric Reliability Corporation (NERC) as the first ever ERO in July 2006, and it has served in that role since.<sup>23</sup> NERC’s mission is to assure the reliability and

---

<sup>18</sup> 16 U.S.C. § 824o, Section (a)(1), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>19</sup> Interconnections are defined as the “geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control.” North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See: “Glossary of Terms Used in NERC Reliability Standards,” *NERC*, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

<sup>20</sup> The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify “local” distribution. See: 16 U.S.C. § 824o, Section (a), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>21</sup> 16 U.S.C. § 824o–1, Section (b)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>22</sup> *Energy Policy Act*, Public Law 109-58, *U.S. Statutes at Large* 119 (2005): pp. 942-943.

<sup>23</sup> NERC, *History of NERC*, August 2013, <http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf>.

For more information on NERC, see: “About NERC,” *NERC*, n.d.a, <http://www.nerc.com/AboutNERC/Pages/default.aspx>.

security of the BPS in North America. As such, NERC will be a key partner in developing template emergency orders, especially to help defeat attacks that could create cascading blackouts or other multi-state disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a critical role for the electric subsector in establishing situational awareness, incident management and coordination, and communication capabilities.<sup>24</sup> E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be particularly vital in consultations on issuing and refining emergency orders against specific threats.

***b. Regional entities responsible for enforcing reliability standards for the bulk power system.***<sup>25</sup> NERC delegates its authority to monitor and enforce compliance with reliability standards to eight regional entities which “account for virtually all the electricity supplied in the United States.”<sup>26</sup> While regional entities play crucial oversight roles, they do not directly operate the grid and would not, on their own, be positioned to execute emergency orders to protect or restore reliability. They will nonetheless play an important role regarding waivers for legal and regulatory compliance, as will be examined in detail in Section IV.

***c. Owners, users and operators of critical electric infrastructure (CEI) or defense critical electric infrastructure (DCEI) within the United States.***<sup>27</sup> When the President declares a grid security emergency, issuing emergency orders to power companies that own and operate generation and transmission assets will offer crucial opportunities to protect grid reliability. In addition, Reliability Coordinators (RCs) will play essential roles in designing and implementing emergency orders. RCs are the entities that constitute “the highest level of authority” for the reliable operation of the bulk electric system.<sup>28</sup> RCs are also responsible for maintaining a “wide

---

<sup>24</sup> “Electricity ISAC,” NERC, n.d.a, <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>25</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177. See also: 16 U.S.C. § 824o, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>26</sup> “Key Players,” *North American Electric Reliability Corporation*, n.d.a., <https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>. One regional entity, however, announced its intention to dissolve in July 2017, currently pending final FERC approval. See: North American Electric Reliability Corporation, “JOINT PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION, MIDWEST RELIABILITY ORGANIZATION, AND SERC RELIABILITY CORPORATION FOR APPROVALS IN CONNECTION WITH THE DISSOLUTION OF THE SOUTHWEST POWER POOL REGIONAL ENTITY,” *Filing Before the Federal Energy Regulatory Commission* (Docket No. RR18-3-000), <https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/SPP%20Dissolution%20Petition.pdf>.

<sup>27</sup> The analysis that follows later in this section examines the definition of “users” of critical electric infrastructure, as well as defense critical electric infrastructure.

<sup>28</sup> While the Bulk Power System (BPS) broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the Bulk Electric System (BES) is a subset of the BPS which includes, with some exclusions, all transmission and real and reactive power sources at 100 kV or higher. As with the BPS, the BES definition excludes local distribution providers. For these definitions, as well as the definition of Reliability Coordinators, see: “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf). Consistent with the FPA and the authorities it provides for



area view” of the bulk electric system, and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, RCs will be critical for designing, receiving, and implementing emergency orders to counter attacks that may exceed the ability of individual BPS system owners and operators to defeat. Seven Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) also help operate and ensure the reliability of the bulk electric system in many regions of the United States.<sup>29</sup> Accordingly, RTOs and ISOs will be essential to the design and execution of emergency orders.

#### ***d. Local Distribution Providers***

The role of distribution systems in responding to grid security emergencies is less clear-cut. As noted above, the Federal Power Act only authorizes the Secretary to issue emergency orders to bulk power system entities. The Act does not explicitly authorize the Secretary to issue emergency orders to utilities that provide for local distribution of electric power. Nevertheless, local distribution infrastructure may play a vital role in protecting the flow of power to key facilities in grid security emergencies. Even if emergency orders can help defeat attacks on the bulk power system, adversaries may still be able to achieve catastrophic effects by attacking multiple local distribution systems, and thereby interrupt the flow of power from transmission systems to hospitals and other end users. A holistic approach to GSE preparedness will need to account for these risks to local infrastructure.

Integrating local distribution systems into planning for grid security emergencies will also be useful from an operational perspective. Even though local distribution utilities may not themselves be subject to EOs, they may be functionally required to help implement such orders. For example, if the Secretary orders transmission systems to shed load to protect grid reliability, while also preserving the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding.

From an historical perspective, it is understandable why the FPA does not explicitly account for local distribution utilities in grid security emergency operations. State public utility commissions have long had regulatory jurisdiction over distribution systems. Any legislative effort to give the Secretary of Energy emergency authorities over local distribution assets could have created strong opposition from state leaders and their defenders in Congress.<sup>30</sup> Nevertheless, if the

---

handling grid security emergencies, this study focuses on the application of emergency orders to BPS entities specifically.

<sup>29</sup> There are 10 RTOs and ISOs under NERC’s purview, though three operate exclusively in Canada. RTOs and ISOs are independent, membership-based, non-profit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are operated by individual utilities or utility holding companies. “About 60% of the U.S. electric power supply is managed by RTOs,” *U.S. Energy Information Administration*, April 4, 2011, <https://www.eia.gov/todayinenergy/detail.php?id=790>. Six of the seven RTOs/ISOs are also current reliability coordinators. See: “Reliability Coordinators,” *North American Electric Reliability Corporation*, n.d.a., <https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.

<sup>30</sup> The U.S. Constitution, in most cases, only allows Federal regulation of private economic activity for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See: Jim Lazar (for The Regulatory Assistance Project), *Electricity Regulation in the US: A Guide*, 2<sup>nd</sup> Edition, June 2016, p. 15.

United States is to prevent grid-wide attacks from jeopardizing national security, economic security, or public health or safety, extensive coordination and collaboration with local distribution systems will be essential.

An initial step toward building such an integrated approach will be to specify which distribution facilities that serve CEI and DCEI are “local.” As FERC notes, the FPA’s BPS definition “does not establish a voltage threshold limit of applicability or configuration.” The definition instead relies on the functional requirement of “necessary for operating an interconnected electric energy transmission network” set out by the FPA.<sup>31</sup>

Local distribution utilities which are not necessary for such interconnected operations may nevertheless provide the “last mile” of power delivery to military bases and other vital facilities. It might be possible to interpret the FPA as making emergency order applicable to these utilities as well. The Act states that emergency orders may apply to “any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure” within the United States. The Act, however, does not further define owners, users and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the Act.

Even if the Secretary cannot issue orders directly to such utilities, BPS entities should still include them in building the contingency plans necessary to implement emergency orders. Before BPS owners and operators receive EOs, they could pre-plan to coordinate with local distribution systems to strengthen comprehensive, end-to-end protection of grid reliability for critical customers. Many companies that own transmission assets also own distribution infrastructure, simplifying coordination for EO planning purposes. Integrated planning will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for “vertically integrated” utilities that own and operate assets for all three functions.

However, while many investor-owned utilities are vertically integrated, municipally-owned electric utilities and rural electric cooperatives (which serve a significant amount of CEI and DCEI) are not. In the many regions of the United States where generation, transmission, and distribution systems exist as separate, non-integrated companies, additional engagement

---

<sup>31</sup> Federal Energy Regulatory Commission, *Revision to Electric Reliability Organization Definition of Bulk Electric System* (Order No. 743), 133 FERC ¶ 61,150, November 18, 2010, pp. 22-24. FERC and NERC have also defined the Bulk Electric System (BES), a subset of the BPS, for regulatory purposes. Unlike the FPA’s BPS definition, NERC’s core BES definition establishes a uniform “bright line” threshold of 100 kV. Accordingly, the BES includes “all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher,” with specific, additional criteria for inclusions and exclusions to provide further clarity. NERC also established an exception process through their Rules of Procedure to make additional inclusions and exclusions on a case-by-case basis. FERC accepted the definition in 2012 (Docket Nos. RM12-6-000 and RM12-7-000; Order No. 773), and the FERC decision was upheld by the Second Circuit Court of Appeals, in *New York V. FERC*, 783 F.3d 946 (2d Cir. 2015). See: Federal Energy Regulatory Commission, *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure* (Order No. 773-A), 143 FERC ¶ 61,053, April 18, 2013, pp. 2-7; and “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

measures will be essential to help effectively implement EOs. As the Federal government identifies critical facilities for prioritized protection and restoration of power, BPS entities that provide the electricity on which those facilities rely should ensure that local distribution systems are included in designing and implementing orders for prioritized emergency service.

#### *e. Additional Partners for Engagement*

As the Department of Energy and the electricity subsector develop emergency orders, they should identify and pre-plan with other partners who can assist in executing those orders. The GSE Rule notes that “Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits” to expedite the restoration of power.<sup>32</sup> Still broader collaboration with government and private sector partners may be valuable for implementing EOs to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy Large Power Transformers (LPTs) at substations across the United States, and these attacks cut off power to critical military bases, the Secretary might order industry to prioritize the replacement of LPTs at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program (STEP) to provide for such replacements,<sup>33</sup> and new industry-led organizations such as Grid Assurance and the Regional Equipment Sharing for Transmission Outage Restoration Agreement (RESTORE – a mutual assistance-like agreement for enabling transfers of transformers and other critical equipment recently approved by FERC).<sup>34</sup> These initiatives further strengthen the industry’s LPT resilience posture in ways that could be valuable for restoration operations in grid security emergencies.

However, power companies do not move LPTs by themselves. They rely on railroad companies, barges, and “heavy hauler” trucking companies to help do so, and have established a Transformer Transportation Working Group (TTWG) to plan and coordinate LPT movement operations.<sup>35</sup> The FPA does not give the Secretary authority to issue orders to transportation companies. Nevertheless, in anticipation of orders for transformer movement, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Pre-coordinating with the U.S. Department of Transportation and state governments to get permits and regulatory waivers to expedite transformer movement will also be helpful.

---

<sup>32</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177.

<sup>33</sup> See: Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>; and “Spare Transformers,” *Edison Electric Institute*, n.d.a, <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.

<sup>34</sup> Federal Energy Regulatory Commission, *ORDER AUTHORIZING ACQUISITION AND DISPOSITION OF JURISDICTIONAL FACILITIES* (163 FERC ¶ 61,005), April 3, 2018, p. 10, <https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf>.

<sup>35</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 12, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

Equally valuable partnership opportunities will emerge in designing and pre-planning for the execution of other emergency orders. For example, when the Secretary issues an emergency order, agencies and utilities should already have determined what they will tell the public about the purpose of the order, its expected impact on electric service, and -- ideally -- when normal service will be restored. Identifying these and other partnership requirements will be critical as the design process goes forward.

### **3. Template Emergency Orders: Goals and Specific Design Requirements**

The starting point to develop template emergency orders is to identify the objectives and design requirements that these orders will need to encompass, and clarify the underlying policy challenges that the EO development process will need to address. Key issues analyzed in the next sections of the study:

- Threats, Triggers and Thresholds for Issuing Emergency Orders. The Federal Power Act requires the President to have declared a “grid security emergency” (GSE) before the Secretary can issue emergency orders.<sup>36</sup> Only a limited number of natural and manmade hazards can trigger a GSE. Countering each of those hazards will require different, threat-specific specific emergency orders. Hence, the first step for developing such orders will be to select the threats on which the design process should focus.

The Act authorizes the President to declare a GSE when there is an “imminent danger” of attacks on critical grid infrastructure, or when attacks are occurring.<sup>37</sup> Different types of emergency orders will be needed to preserve grid reliability 1) when attacks are imminent, and 2) when attacks are underway. Promising opportunities also exist to develop orders for a third phase of GSE operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.

- Incorporating National Security Policies and Priorities into GSE Order Design. The FPA’s definition of grid security emergencies helps frame the order design process in an additional way. GSEs exist when adversaries pose serious threats to:
  - *Critical electric infrastructure*, which is comprised of grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters;”<sup>38</sup> and
  - *Defense critical electric infrastructure*, which serves facilities that are “critical to the defense of the United States” and are vulnerable to the disruption of grid-provided power.<sup>39</sup>

---

<sup>36</sup> Along with cyberattacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>37</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>38</sup> 16 U.S.C. § 824o–1, Section (a)(2), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>39</sup> 16 U.S.C. § 824o–1, Section (a)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

Government and industry partners should design emergency orders to protect and restore the reliability of these high-priority grid systems and the customers they serve.

Emergency orders should also reflect broader Federal government strategies to defend critical infrastructure. The U.S. *National Security Strategy*, for example, provides crucial guidance on how the United States will deter attacks on critical systems, and -- if deterrence fails -- defeat the attackers.<sup>40</sup> DOE and its industry partners should design emergency orders to help implement the Strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this strategic design process with two further steps. First, building on the provisions of the FPA and on existing industry plans to prioritize the restoration of power, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement EOs and help defend the nation.

- Communications. The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The Rule on Procedures for Issuance of emergency orders (hereinafter referred to as the ‘GSE Rule’) provides a description of the consultative process that (if practicable) will occur before the Secretary sends such orders.<sup>41</sup> However, the GSE Rule does not address the risk that adversaries will attack the industry-government communications systems necessary to issue orders, monitor their compliance, and defeat adversary attacks. Building secure, survivable communications will be essential to the effective use of emergency orders to protect or restore grid reliability. However, the FPA establishes no requirements or funding to do so. Industry and government partners should consider including secure communications as a crucial component of the overall GSE preparedness effort, lest those potential vulnerabilities be left for adversaries to exploit.

Government and utility leaders will also need to coordinate what they tell the American people when the Secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including EOs for prioritized load shedding, could cut off electricity to many thousands of customers in order to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by pre-planned communications playbooks to address customer concerns.

Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Adversaries will strike the grid to achieve

---

<sup>40</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 13.

<sup>41</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1181.



political benefits, including, potentially, the incitement of public panic and a loss of confidence in U.S. leaders. Building upon existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders, will be essential to provide for unity of messaging against such efforts.

- Waivers and Cost Recovery. Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the Act, FERC-approved reliability standards, or environmental regulations.<sup>42</sup> However, potentially valuable emergency orders will be easier to implement if they include pre-planned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.<sup>43</sup> Industry-government dialog will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader pre-planning needed for the financial challenges that grid security emergencies could create, including the catastrophic loss of power company revenue and the breakdown of company access to emergency loans or other financial instruments.

## **II. THREATS, TRIGGERS, AND CONSULTATIVE OPTIONS FOR DECLARING GRID SECURITY EMERGENCIES**

The Federal Power Act leaves the President substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should also consider seeking consensus on the types of threats that on which the development process should focus, and establish decision criteria and consultative mechanisms to support GSE declarations.

### **A. THREATS THAT CAN TRIGGER GRID SECURITY EMERGENCIES: IMPLICATIONS FOR EO DESIGN**

A broad array of natural and manmade hazards can cause multi-state blackouts, including earthquakes and severe weather events such as hurricanes and ice storms. However, in amending the Federal Power Act, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the “occurrence or imminent danger” of:

- 1) “A malicious act using **electronic communication** or an **electromagnetic pulse**, or a **geomagnetic storm** event, that could disrupt the operation of those electronic devices or

---

<sup>42</sup> These waivers apply unless companies carry out orders and related actions in a “grossly negligent manner.” See: 16 U.S.C. § 824o-1, Section (f)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>43</sup> 16 U.S.C. § 824o-1, Section (b)(6), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;”<sup>44</sup> and

2) “Disruption of the operation of such devices or networks, with significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event;” or

3) “A **direct physical attack** on critical electric infrastructure or on defense critical electric infrastructure;” and

4) “Significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.”<sup>45</sup>

Protecting CEI and DCEI against each of these threats will require different types of emergency orders. The threats will also pose disparate challenges for determining the imminence or occurrence of a grid security emergency, ranging from relatively simple to deeply problematic. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the President faces uncertainties about the likelihood and potential consequences of a GSE.

### **1. Geomagnetic Storms as a Possible Initial Focus**

Emergency orders against geomagnetic disturbances (GMD) will entail fewer design challenges than for cyberattacks and other manmade hazards, and could therefore provide opportunities for relatively rapid progress in strengthening GSE preparedness. GMD events occur when coronal mass ejections on the sun create geomagnetically induced currents (GICs) on the surface of the earth. These currents can damage unprotected transformers and other grid infrastructure. Compared to the other threats that can trigger grid security emergencies, determining that there is an imminent danger of a GMD event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the President decide whether to declare a GSE, and will provide hours of warning before the solar energy begins creating destructive GICs.

Industry and government partners can develop emergency orders that exploit this warning time. For example, the Secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of ground induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.<sup>46</sup>

---

<sup>44</sup> Section II of this paper defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of GSE thresholds.

<sup>45</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>46</sup> Dr. Tony Phillips, “Solar Shield--Protecting the North American Power Grid,” NASA, October 26, 2010, [https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\\_solarshield](https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield). See also: MISO, *Geomagnetic Disturbance Operations Plan* (SO-P-AOP-01 Rev: 1), June 9, 2017, p. 5, <https://www.misoenergy.org/Library/Repository/Procedure/SO-P-AOP-01%20Geomagnetic%20Disturbance%20Operations%20Plan.pdf>.

A strong foundation already exists for drafting such orders. Studies of GMD effects on the power grid have generated a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.<sup>47</sup> Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the Federal Government to ensure that it has the capability to predict and detect space weather events, the ability to communicate these assessments to public and private sector stakeholders, protection and mitigation plans for critical infrastructure, and response and recovery plans for GMD events. The order requires Sector-Specific Agencies to “assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event.”<sup>48</sup> NERC standards also exist for addressing GMD threats. TPL-007-1 – *Transmission System Planned Performance for Geomagnetic Disturbance Events* establishes long-lead GMD planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat (DBT) for GMD events.<sup>49</sup> EOP-010-1 – *Geomagnetic Disturbance Operations* also requires Reliability Coordinators to develop GMD mitigation plans and operating procedures, including specific actions that Transmission Operators must take based on predetermined GMD-related conditions.<sup>50</sup>

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyberattacks and other manmade triggers for grid security emergencies. The sun will not intentionally hide preparations for a GMD event or “prepare the battlefield” by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data utility personnel need to maintain situation awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of CEI and DCEI.

The relative ease of drafting orders for geomagnetic disturbances makes such GMD efforts a prime starting point for industry-government collaboration. The North American Transmission Forum (NATF), in coordination with the ESCC, is already examining opportunities to develop template emergency orders for GMD events. But the greater degree of difficulty associated with

---

<sup>47</sup> See: National Oceanic and Atmospheric Administration, *NOAA Space Weather Scales*, April 2011, <https://www.swpc.noaa.gov/sites/default/files/images/NOAAscales.pdf>; Metatech (for Oak Ridge National Laboratory), *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*, January 2010, [https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc\\_meta-r-319.pdf](https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf).

<sup>48</sup> The White House, *Executive Order -- Coordinating Efforts to Prepare the Nation for Space Weather Events*, October 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events>.

<sup>49</sup> NERC, *TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events*, December 2014, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States).

<sup>50</sup> The standard, however, does not explicitly lay out what those predetermined conditions should be. See: NERC, *EOP-010-1 – Geomagnetic Disturbance Operations*, June 2014, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States). For an example of GMD plans, see: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, pp. 69-71.

protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of EOs to counter such threats. Instead, DOE and its industry partners should consider pursuing a multi-track development process: at the same time that they seek rapid progress on emergency orders for GMD, they should *immediately* accelerate the long-lead work that will be required against each of the manmade threats that can trigger grid security emergencies.

## **2. Cyber and Physical Attacks**

This study focuses on supporting the development of EOs to protect and restore grid reliability against cyberattacks. The U.S. *National Security Strategy* highlights the imperative to counter the intensifying cyber threats to the grid and other critical infrastructure. The Strategy warns that the vulnerability of U.S. critical infrastructure to cyberattacks and other threats “means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and communications.” Cyber weapons also “enable adversaries to attempt strategic attacks against the United States – without resorting to nuclear weapons – in ways that could cripple our economy and our ability to deploy our military forces.”<sup>51</sup> An immediate focus for EO development efforts should be to help counter such potentially devastating cyber threats, by designing orders to protect or rapidly restore electric service to military bases and civilian-owned facilities vital to the economy and public health and safety.

This study also examines the development of emergency orders against physical attacks on the grid. Since the carefully coordinated attack against the Metcalf, California substation in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high powered rifles or other weapons.<sup>52</sup> Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

Launching physical attacks would entail risks to the adversary beyond those created by cyberattacks. Blowing up transformers and -- potentially -- killing workers who are transporting replacement equipment would immediately escalate conflict with the United States into open kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries will hide on utility networks, arming and pre-positioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

---

<sup>51</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, pp. 12 and 27, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

<sup>52</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation’s Electricity System: Second Installment of the QER*, January 2017, p. 4-34; NERC, *CIP-014-02: Physical Security*, effective October 2, 2015, <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.

Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk-reward calculus in our favor. If EOs can help power companies protect their systems from physical attacks, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Grid owners and operators are also strengthening their preparedness against combined cyber-physical attacks. Such combined attacks can create synergistic disruptions of the grid beyond those from cyber or physical attacks on their own. For example, as in the response to the cyberattacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.<sup>53</sup> Attacks that physically destroy critical components at those substations or shoot utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

To prepare against such difficult challenges, the largest-scale exercise conducted by NERC and the electricity subsector, GridEx, uses combined cyber-kinetic attacks on power companies in multiple U.S. regions as the exercise's scenario. GridEx also assumes that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging far more difficult than in any past U.S. power outage.

This study adopts a similarly severe threat for analyzing possible EOs. In particular, the study examines how orders can protect or restore grid reliability against the combined use of cyber weapons, kinetic strikes, and information warfare against critical electric infrastructure and defense critical electric infrastructure. Of course, separate types of emergency orders will be required against physical and cyberattacks. Orders to deploy additional armed guards to substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead and accounting for the risk of combined attacks will provide valuable context for the development of physical and cyber EOs, and for the public communications support they will require.

The study does not examine options for developing emergency orders against electromagnetic pulse attacks. EMP threats pose a significant potential risk to the grid, and a growing number of utilities are hardening their critical systems against EMP effects.<sup>54</sup> The Department of Energy's EMP strategy provides a valuable framework approach for managing the risks that EMP threats

---

<sup>53</sup> E-ISAC and SANS-ICS, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, March 2016, p. v.

<sup>54</sup> In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to GMDs. The early-time (E1) component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See: Electric Power Research Institute, *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research* (3002000796), December 2013, pp. 3-3-3-4.



pose to the grid and other energy systems.<sup>55</sup> The Department of Homeland Security’s EMP strategy does the same for a broad range of infrastructure sectors.<sup>56</sup> However, significant research will still be required to understand the combined effects of EMP wave components on grid hardware and system-wide operations, and on cost-effective mitigation options and preparedness planning.<sup>57</sup> As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

## **B. THRESHOLDS FOR DECLARING GRID SECURITY EMERGENCIES**

The President can declare a grid security emergency when there is either imminent danger of an attack or when attacks are already occurring.<sup>58</sup> These two circumstances for declaring a GSE will require distinct, sequential types of emergency orders: 1) pre-attack orders to “raise the gates” against imminent cyber and/or physical strikes; and 2) orders to protect grid reliability once attacks are underway, including measures to prevent the spread of cascading failures across critical and defense critical electric infrastructure. DOE and its partners should also consider developing specialized EOs for a third phase of grid security emergencies: operations to accelerate the restoration of power after adversaries have inflicted major blackouts.

Before attacks occur, pre-emptive orders could help grid owners and operators initiate *conservative operations* to reduce the vulnerability of their systems to attack, increase power reserves, and take other measures to manage the grid instabilities that adversaries may seek to create. Power companies already have extensive experience in employing conservative operations (COs) when hurricanes or other severe weather events are approaching. This experience provides a strong foundation on which to develop COs against cyber and physical attacks. However, determining that attacks are imminent can be vastly more difficult than assessing whether a hurricane will strike, especially if adversaries seek to achieve surprise.

A strong foundation also exists to build emergency orders for attacks that are underway. Most important, BPS entities already have plans and capabilities in place to protect grid reliability when major disturbances occur, and reduce the risk that such disturbances will create cascading failures or other widespread disruptions of electric service.<sup>59</sup> For example, NERC already

---

<sup>55</sup> The Department of Energy has set strategic goals for addressing EMP threats, and created an action plan to meet those goals. Department of Energy, *Electromagnetic Pulse Resilience Action Plan*, January 2017; The FY17 NDAA directed DHS to create a similar strategy, which is currently in draft form. “National Defense Authorization Act for Fiscal Year 2017,” Public Law 114-328, *U.S. Statutes at Large* 130 (2016): pp. 2685-2687; and the Electric Power Research Institute (EPRI) continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs* (3002008999), September 2016.

<sup>56</sup> Department of Homeland Security, *Strategy for Protecting and Preparing the Homeland Against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*, forthcoming (Spring 2018).

<sup>57</sup> Idaho National Laboratory, *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*, January 2016.

<sup>58</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>59</sup> The section that follows examines how NERC’s definition of “Adequate level of Reliability” for the Bulk Power System, including the prevention of cascading failures, can be used to help build design standards for emergency order and thresholds for declaring grid security emergencies. North American Electric Reliability Corporation,

requires transmission operators to be able to shed load (i.e., temporarily curtail or cut off electric service to customers) to mitigate operational emergencies.<sup>60</sup> Emergency orders should be developed for equivalent *extraordinary measures* to protect grid reliability.

A third category of emergency orders will also be valuable if (despite such extraordinary measures) attackers are able to create blackouts that jeopardize public health and safety, the U.S. economy, or national security. Electric industry stakeholders should design EOs to *accelerate restoration* of power to critical electric infrastructure and defense critical electric infrastructure if these blackouts occur. The Secretary could also issue such orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these customers. But lists that identify other national security-related assets, including components of the Defense Industrial Base and transportation infrastructure essential for deploying and sustaining military forces abroad, may be closely held by DOD and not yet included in industry restoration priorities. This study will examine how DOE and its industry partners can leverage existing government schemes for identifying critical facilities to help develop and execute EOs for restoration support, and how that sensitive data can be shared with power companies while remaining protected from adversaries.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, EOs for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are underway. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies “stop the bleeding” from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are underway.<sup>61</sup>

DOE and its partners will need considerable flexibility to deal with overlapping GSE phases in designing, issuing, and implementing executive orders. Nevertheless, being able to “rack and stack” potential orders in terms of when they would be issued and which phases of emergency operations they would support can help facilitate a structured, integrated approach to EO development.

---

“Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013.

<sup>60</sup> North American Electric Reliability Corporation, *EOP-011-1: Emergency Operations*, effective April 1, 2017, R1.2.5, [https://www.nerc.com/\\_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).

<sup>61</sup> In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is full restored to pre-event conditions) as the “New Normal” – characterized by “degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months.” See: North American Electric Reliability Corporation, *Severe Impact Resilience: Considerations and Recommendations*, May 9, 2012, pp. 14 and 16.

## **1. Determining When Attacks are Imminent: Criteria for Declaring GSEs and Issuing Emergency Orders**

The Federal Power Act defines GSEs as occurring when attacks that are imminent or underway “could disrupt the operation” of devices or networks that are “essential to the reliability of critical electric infrastructure or defense critical electric infrastructure.”<sup>62</sup> But the Act does not define imminent. Nor does it clarify the degree of potential disruption that will trigger the declaration of a GSE or detail the criteria that the President should use to make such a decision.

In key respects, the BPS system is under cyberattack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant APTs on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS systems, secrete malware designed to disrupt grid operations, and conduct other malicious activity to prepare for possible attacks on critical system components.<sup>63</sup> PJM Interconnection’s former CEO, Terry Boston, said the RTO experiences 3,000-4,000 hacking attempts *every month*.<sup>64</sup> Penetration efforts on a similarly massive scale are likely to be occurring against BPS entities across the United States. And, as in the case of Black Energy and other adversary campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.<sup>65</sup>

The President could conceivably decide that such campaigns constitute “occurring” attacks under the FPA that should trigger the declaration of a grid security emergency (and, presumably, the use of appropriate countermeasures against the perpetrator). Alternatively, the President might take these measures as evidence that there is “imminent danger” of an attack, and declare a GSE before adversaries used embedded malware to disrupt the operation of devices or networks essential to the reliability of CEI or DCEI.

Federal decision makers could also decide to set the threshold much higher. For example, the President might only declare a grid security emergency if adversaries were poised to disrupt CEI and DCEI across multiple regions of the United States, and could sustain those disruptions for a week or more. The text of the Federal Power Act leaves substantial ambiguity over the criteria that should trigger a GSE and justify the issuance of issue emergency orders to protect grid

---

<sup>62</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>63</sup> “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Readiness Team*, March 15, 2018, <https://www.us-cert.gov/ncas/alerts/TA18-074A>; “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Response Team (US-CERT)*, October 20, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-293A>; Defense Science Board, *Task Force on Cyber Deterrence*, February 2017, p. 4; ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*, June 2016, p. 19.

<sup>64</sup> Jon Dougherty, “Biggest U.S. power grid operator suffers thousands of attempted cyber attacks per month,” *Forward Observer*, August 22, 2017, <https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/>.

<sup>65</sup> Black Energy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of Black Energy inflicted the 2016 blackout on Ukraine. Alert (ICS-ALERT-14-281-01E), “*Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*, last updated December 9, 2016, <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.

reliability. In an intense crisis, this ambiguity could fuel disagreements amongst the President's advisors as to whether the threat of attack was sufficiently severe to declare a GSE, and unleash the firestorm of media speculation and congressional concern that a public declaration would produce.

But it would be a mistake to adopt a rigid set of GSE thresholds. Preserving broad latitude for the President to determine what constitutes a GSE will provide flexibility to deal with unforeseen circumstances and help avoid locking U.S. crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicly draw explicit "red lines" that would trigger a GSE. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay U.S. defensive measures, including the issuance of emergency orders to protect grid reliability. Adversaries might even seek to "spoof" the President into declaring a GSE when they had no intention of launching an attack – especially if doing so might incite public panic that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events which emergency orders should be designed to help counter. One option for clarifying such thresholds is to focus on the geographic scope of an emergency. In responding to DOE's *Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance*,<sup>66</sup> the ISO-RTO Council proposed that the use of emergency orders "should be reserved for true widespread emergencies." Equivalent criteria might be created by the President's advisors to support internal deliberations on whether to declare a GSE. However, additional options exist to assist such decision making in ways that are better attuned to the purposes of the Federal Power Act and offer more direct value for developing emergency orders.

## **2. Preventing Cascading Blackouts, Uncontrolled Separation, and other Disruptions of "Adequate Levels of Reliability"**

The North American Electric Reliability Corporation (NERC) has carefully defined what constitutes adequate reliability for the power grid, and the types of large-scale failures in reliability that owners and operators need to prevent. The imminent danger or occurrence of such failures should almost certainly be considered sufficient to declare a grid security emergency. The technical and operational requirements needed to prevent these failures also provide an opportunity to tailor emergency orders for each of them.

The 2003 Northeast blackout spurred efforts to define an adequate level of reliability for the grid and the system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over major portions of the United States, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The

---

<sup>66</sup> Theodore J. Paradise et al., "ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance—RIN 1901–AB40," *ISO-RTO Council*, February 6, 2017, [http://www.isorto.org/Documents/Report/20170206\\_Final\\_IRC-DOE\\_NOPR\\_Comments\\_re\\_Grid\\_Security\\_Emergency.pdf](http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf).

2005 amendments required FERC to certify an Electric Reliability Organization (ERO), which will have “the ability to develop and enforce ... reliability standards that provide for an adequate level of reliability of the bulk-power system.”<sup>67</sup> However, the EPA never defined “adequate level of reliability” (ALR); that task was left to the ERO to complete.

When NERC became the ERO in 2006, defining the ALR became one of its first initiatives. NERC’s Board of Trustees approved an initial definition for the “characteristics of a system with an adequate level of reliability” in 2008.<sup>68</sup> In May 2013, NERC released an updated ALR definition.<sup>69</sup> Three components of NERC’s definition are especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS, and to clarify the scale and scope of threats that EOs should be designed to counter.

The sections that follow examine each of these three components and the failures in reliability they can entail. However, in severe events, all three types of failures often occur in rapid succession and are inextricably linked. Protecting against their combined effects will be a key challenge in preparing for grid security emergencies.

**a. Instability.** NERC defines system instability as “the inability of the Transmission system to remain in synchronism ... characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES.”<sup>70</sup> The BES can experience frequency, voltage, or angular instability – though none should occur during normal operating conditions.<sup>71</sup>

Temporary instabilities occur occasionally; grid protection systems and operational protocols typically protect the bulk power system, mitigating their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, if BES generators accelerate or decelerate too much during a disturbance, the Transmission system may experience large power swings, causing transmission lines to trip and/or generators to go out of step and trip offline, resulting in further acceleration and deceleration.<sup>72</sup> Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread, cascading failures across CEI and DCEI. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur, given the speed at which instabilities propagate. Though difficult to predict, the determination that attackers were poised to both create instabilities and

---

<sup>67</sup> *Ibid.*

<sup>68</sup> North American Electric Reliability Corporation, *Technical Report Supporting Definition of Adequate Level of Reliability*, March 26, 2013, p. 17.

<sup>69</sup> The document refers to the Bulk Electric System (BES) rather than the Bulk Power System (BPS). See note 25 on differences between NERC’s BES and BPS definitions. Again, for the sake of clarity and consistency with the FPA this study uses the term BPS throughout.

<sup>70</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, p. 6.

<sup>71</sup> *Ibid.*, at pp. 1-2.

<sup>72</sup> *Ibid.*, at 6.



nullify protective systems could provide an additional basis for declaring a grid security emergency. Industry and government partners should explore the development of emergency orders for conservative operations to give the Transmission system extra “slack” to (ideally) avoid instabilities, as well as for extraordinary measures to help the system remain in synchronism should major instabilities occur.

**b. Cascading Failures.** NERC defines cascading as “the uncontrolled successive loss of system elements triggered by an incident at any location.” Such cascading “results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.”<sup>73</sup> NERC’s definition of the Adequate Level of Reliability (ALR) for the BPS states that the system will not experience cascading when struck by lightning strikes and other frequent, predictable incidents (i.e., “predefined Disturbances”). But more severe events have caused instabilities which led to cascading in the past and may do so again – especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout was especially wide-ranging and spurred the development of mandatory reliability standards to reduce the risk of such failures in the future. That blackout (which affected approximately 50 million people across the U.S. and Canada) started with a relatively minor incident. On a hot day in August, multiple 345-kV transmission lines tripped after sagging into overgrown trees. While operator actions might have been able to handle such a contingency with proper situational awareness, failures in the utility’s control room alarm processor resulted in operators being unaware of the problem entirely. In an extremely unfortunate coincidence, the utility’s Reliability Coordinator also had computer problems and was lacking the visual tools necessary to provide support.<sup>74</sup> These failures shifted power flows to a system of 138-kV lines which were unable to handle the added current flows, also overloading the last remaining 345-kV path into the area, and beginning the major, uncontrollable cascading sequence.<sup>75</sup> This sequence tripped over 500 generating units and 400 transmission lines in only eight minutes – most of which actually occurred *in the last 12 seconds* of the cascade.<sup>76</sup>

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversary attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying key generation and transmission nodes; altering protective relay settings so that grid components trip off line (or fail to do so) in ways that intensify the outages; denying grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and taking other measures designed to produce cascading failures.<sup>77</sup>

---

<sup>73</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, pp. 1 and 7.

<sup>74</sup> North American Electric Reliability Corporation, *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?*, July 13, 2014, pp. 27-28.

<sup>75</sup> *Ibid.*

<sup>76</sup> North American Electric Reliability Corporation, *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?*, July 13, 2014, p. 109.

<sup>77</sup> Anton Cherepanov and Robert Lipovsky, “Industroyer: Biggest threat to industrial control systems since Stuxnet,” *ESET Blog: WeLiveSecurity*, June 12, 2017, <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat->

Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe – particularly by undermining situational awareness data and capabilities.

The imminent danger or occurrence of adversary-induced cascading outages could be criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt the operation of grid devices and networks essential to CEI and DCEI – and do so on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

As will be discussed in Section III, it may be difficult to determine that an impending attack poses an imminent danger of creating cascading failures given the technical challenges of predicting the systemic effects of cyber and physical strikes. Waiting until an attack is underway to assess the risks of cascades will also pose challenges. As in 2003, failures can spread across vast areas in seconds, and adversaries may seek to disrupt grid operators’ situational awareness. Nevertheless, given the threat that cascading blackouts would pose to CEI and DCEI, any significant risk that adversaries are poised to create such effects should be sufficient to declare a grid security emergency.

Promising opportunities also exist to develop emergency orders to reduce the risk of cascading failures. Emergency load shedding provides one such opportunity. After action reports from the 2003 blackout found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. In particular, a U.S.-Canada task force found that “Timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio.”<sup>78</sup> In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.<sup>79</sup>

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for Transmission Operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation on which to build emergency orders to reduce the risk that physical and cyberattacks will create cascading blackouts, and – potentially – tailor EOs and implementation plans to exclude vital facilities from load shedding.

---

industrial-control-systems-since-stuxnet/; Chris Sistrunk, “ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One),” *SANS Industrial Control Systems*, January 8, 2016, <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>; *United States Computer Emergency Readiness Team*, “Alert (TA17-163A): CrashOverride Malware,” June 12, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-163A>; Dragos, Inc, *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*, June 13, 2017, p. 24.

<sup>78</sup> U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 147.

<sup>79</sup> *Ibid.*, at p. 77.

**c. Uncontrolled Separation.** NERC defines uncontrolled separation as “the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss.”<sup>80</sup> Severe events “resulting in the removal of two or more BES elements with high potential to cascade” can produce uncontrolled separation.<sup>81</sup>

Uncontrolled separation almost always occurs following cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands which “quickly became unstable after the massive transient swings and system separation” because there was insufficient generation within the island to meet electricity demand.<sup>82</sup> Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.<sup>83</sup> In the 1982 West Coast blackout, loss of 500-kV lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, and separation of the system into four unplanned islands.<sup>84</sup> A similar blackout in the same region in 1996 triggered by multiple major transmission line outages, the Western Interconnection again separated into four electrical islands “with significant loss of load and generation.”<sup>85</sup>

Unplanned islands are inherently unstable. Uncontrolled separation only rarely (and near-miraculously) produces synchronous islands in which load and generation are balanced within their perimeters.<sup>86</sup> A better way to produce stable islands may be to pre-plan for them. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, pre-planned islands might become a hedge against cascading failures and uncontrolled separation. In practice, such islanding will entail immense technical and operational problems. Section IV provides a detailed analysis of these opportunities and challenges.

Taken together, these criteria for maintaining grid reliability could constitute “high level” thresholds for declaring GSEs. If the Bulk Power System faced an imminent threat of cascading blackouts, uncontrolled separation, or widespread instability, the potential consequences for the U.S. economy and national security would be so severe that declaration of a GSE should be near-automatic.

However, systemic threats to grid reliability are far from the only criteria that the President might want to consider. Much more narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security – including the National Capital Region – might be

---

<sup>80</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, p. 6.

<sup>81</sup> *Ibid.*, at p. 13.

<sup>82</sup> U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 75.

<sup>83</sup> *Ibid.*, at p. 104.

<sup>84</sup> *Ibid.*, at p. 105.

<sup>85</sup> *Ibid.*, at p. 106.

<sup>86</sup> National Academy of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation’s Electricity System* (Washington D.C.: The National Academies Press, 2017), p. 81.

sufficient to declare a grid security emergency. The President should retain adequate flexibility to make such declaration across a broad range of contingencies. Developing emergency orders to protect and restore service to such critical areas should be a priority as well, together with orders to prevent cascading failures across larger portions of the United States.

### **3. Further Options to Support GSE Declarations: Attack Consequences, Geopolitical Circumstances, and Adversary Efforts to “Prepare the Battlefield”**

Additional criteria can help clarify thresholds for declaring GSEs and for issuing emergency orders while providing such latitude. One criterion is the potential impact of attacks on U.S. national security, the economy, and public health and safety. As noted above, the FPA defined GSEs as occurring when attacks “could disrupt the operation” of CEI or DCEI.<sup>87</sup> Policymakers should consider refining that overly broad standard by leveraging the definition of “significant cyber incidents” in Presidential Policy Directive-41 (PPD-41), *United States Cyber Incident Coordination*. Under PPD-41, “significant cyber incident” are those that are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.”<sup>88</sup> That demonstrable harm standard can help set an appropriately high bar for declaring GSEs and issuing EOs

For determining that attacks are imminent, decision makers might also take the geopolitical climate into account. It is (barely) conceivable that adversaries will launch a “bolt from the blue” attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region, and attack the grid to disrupt the deployment of U.S. forces to the region or achieve other military and political goals.<sup>89</sup> Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause demonstrable harm via grid attacks, should carry greater weight in crises than in peacetime.

The emergence of a regional crisis would also provide opportunities to intensify and specially target searches for destructive malware. Industry and government should ensure that as tensions rise, agencies are already prepared to ramp up intelligence sharing with BPS entities, especially in terms of specific malware signatures to search for in utility networks, data logs, and critical equipment. Pre-attack emergency orders could help facilitate such intensified collaboration.

Gathering and sharing data on adversary efforts to prepare the battlefield can also support GSE determinations. DOE and its industry partners have taken major strides to improve such sharing;

---

<sup>87</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>88</sup> White House, *Presidential Policy Directive - United States Cyber Incident Coordination*, July 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

<sup>89</sup> Section II C examines these national security-related issues and their implications for designing emergency orders.

especially on the operational technology networks (OT) and other systems that help control grid operations. For example, DOE's Cybersecurity Risk Information Sharing Program is a public-private partnership to build bi-directional situational awareness and facilitate classified and unclassified information sharing.<sup>90</sup> The CRISP is managed by the E-ISAC, which plays an integral role in establishing situational awareness in the electricity subsector. The E-ISAC is also central to electric industry incident coordination efforts, including cybersecurity threat assessments and sharing incident data.<sup>91</sup>

Advancing the ability to improve situational awareness of OT networks is a key focus of DOE's current activities. The Department is currently in the early stages of taking the lessons learned from CRISP and developing an analogous capability to monitor traffic on OT networks via the Cybersecurity for the Operational Technology Environment (CYOTE) pilot project. Observing anomalous traffic on networks – and having the ability to store and retrieve network traffic from the recent past – can be the first step in stopping an attack in its early stages.

The President's advisors may want to employ additional technical criteria in making pre-attack GSE determinations. One opportunity lies in using the Industrial Control System (ICS) Cyber Kill Chain, which identifies the specific, sequenced phases that adversaries execute in order to conduct attacks that inflict predictable physical effects on grid equipment and operations.<sup>92</sup> Stage 1 begins with planning and reconnaissance against ICS networks, and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing capabilities to attack ICS networks, and – ultimately – executes the attack. Evidence of an adversary's position along this Kill Chain could help support decision-making on the imminence of potential threats, with the final phases posing the most proximate risks of attack.

Another option lies in using established Federal cyber incident criteria. For example, consistent with PPD-41, *United States Cyber Incident Coordination* (July 2016), the National Cyber Incident Response Plan (NCIRP) issued in December 2016 provides a Cyber Incident Severity Schema to serve as “a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments” and agencies.<sup>93</sup> Appendix A provides the Schema. As efforts go forward to refine the Schema and the NCIRP, significant opportunities will exist to crosswalk and provide for consistency between such Federal Government-wide assessment systems and possible GSE thresholds for internal use by the President and supporting staff and departments.<sup>94</sup>

---

<sup>90</sup> “Energy Sector Cybersecurity Preparedness,” *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

<sup>91</sup> “Electricity ISAC,” *NERC*, n.d.a., <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>92</sup> The ICS Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin in 2011 to “help the decision-making process for better detecting and responding to adversary intrusions.” The ICS Cyber Kill Chain tailors that decision-making tool for ICS-specific cyber threats and consequences. See: Michael Assante and Robert M. Lee, “The Industrial Control System Cyber Kill Chain,” *SANS Institute*, <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.

<sup>93</sup> Department of Homeland Security, *National Cyber Incident Response Plan*, December 2016, pp. 29-30.

<sup>94</sup> One option would be to explicitly link the declaration of a GSE to the designation of a cyber incident as a “Level 5 Emergency,” which poses “an imminent that to the provision of wide-scale critical infrastructure services, national government stability, or to the lives of U.S. persons.” But other Schema levels (either lower, or, potentially, higher if



Of course, an enormous difference exists between making preparations for an attack and actually launching one. But if adversaries were to suddenly move to the penultimate phase of stage 2 (delivery and installation of the attack capability) during an intense political crisis or regional confrontation, evidence that they had taken such a move could help support GSE decision-making. Gathering such evidence against sophisticated attackers may require sustained improvements in sensors and OT/IT system monitoring.

### **C. PRE-ATTACK GSE DECLARATIONS: OPTIONS FOR DATA SHARING AND CONSULTATION WITH INDUSTRY**

Decisions regarding pre-attack GSE declarations would benefit significantly from thorough industry consultation. However, neither the Federal Power Act nor the *Final Rule on Grid Security Emergency Orders: Procedures for Issuance* explicitly provide for such discussions. The GSE Rule specifies that “before an emergency order is put into effect and, to the extent practicable and in light of the nature of the grid security emergency and the urgency of the need for action, efforts will be made to consult” with the ESCC, the owners, users and operators of CEI and DCEI, and other resilience stakeholders.<sup>95</sup> DOE might benefit from making equivalent commitments to seek industry input on the declaration of GSEs.

Only power companies will have access to the precursory malware that adversaries implant on their networks, as well as unique expertise in assessing the potential impact of the malware on their systems if attacks begin. Government leaders should consider consulting with BPS entities before the President declares a GSE so that the President’s advisors can benefit from their technical perspectives, and so that government and industry can jointly prepare for the media turmoil that a declaration will almost certainly produce.

As with consultations on issuing orders, urgent circumstances could foreshorten or preclude opportunities for government dialog with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of “bolt from the blue” attacks. However, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be extraordinarily valuable in determining whether (and when) to declare a grid security emergency. Now is the time to explore options to coordinate such discussions, preferably by leveraging existing consultative mechanisms under the ESCC and E-ISAC.

### **III. A FRAMEWORK FOR DEVELOPING EMERGENCY ORDERS: GSE PHASES AND ORDER DESIGN OPTIONS**

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal with these ambiguities is to delay the

---

additional categories are developed) could provide for such linkages. Department of Homeland Security, *National Cyber Incident Response Plan*, December 2016, p. 38.

<sup>95</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1181.

declaration of a GSE until blackouts begin, foregoing the benefits of issuing pre-attack emergency orders. Industry and government partners should instead explore options to design EOs for the Secretary to issue when risks of cyberattack are elevated – especially if such orders will have little or no disruptive effects on normal grid service. These partners should also develop more extreme and potentially disruptive options for use when attacks are underway and when restoration operations begin.

## **1. Pre-Attack Options**

Conservative operations that utilities implement against natural hazards help illuminate the value that pre-attack EOs could offer against manmade threats. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects, and prepare for possible response and restoration operations if grid infrastructure is damaged.<sup>96</sup> For example, Reliability Coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.<sup>97</sup> Power companies may also cancel non-critical generation and transmission maintenance activities and staff their back-up control centers, critical BPS substations, and other key facilities to set the stage for emergency operations as hurricanes approach.<sup>98</sup>

A key feature of these frequently-used conservative operations (COs) is that they do not disrupt normal service to customers. The negligible impact of these COs on day-to-day service helps make them more viable for a utility to implement when the storm's path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the U.S. coast. Instead, they provide a wide “cone of uncertainty” that becomes increasingly narrow as the hurricane approaches. However, utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other COs. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these COs do not affect normal service to customers enhances the willingness of utility leaders to order their implementation amidst the uncertainty.

---

<sup>96</sup> Conservative operations are not defined in the NERC Glossary of Terms. However, many Reliability Coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken “to implement additional actions to ensure the BES [Bulk Electric System] remains reliable in the face of the additional threats” when “events, conditions, or circumstances may put the [BES] at an increased level of risk, compared to normal operating conditions.” See: PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 3, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>. Similarly, the Western Electricity Coordinating Council, defines Conservative Systems Operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets “Are restricted and managed in order to maintain or the restore reliability of the power system from the negative influence of a triggering event or condition.” See: Western Electricity Coordinating Council, *Conservative System Operations* (training slides, n.d.a.), p. 4, [https://www.wecc.biz/Administrative/ProviderXXX\\_CSO\\_20XX\\_Presentation.pdf](https://www.wecc.biz/Administrative/ProviderXXX_CSO_20XX_Presentation.pdf).

<sup>97</sup> PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 3, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.

<sup>98</sup> PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 9, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.

Industry and government partners should borrow from this model to develop orders for pre-attack conservative operations against cyber and/or physical attacks. As a regional confrontation or other precipitating crisis intensifies, it is possible (though unlikely) that the U.S. intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. Instead, based on evidence gathered on utility networks and other sources, the President may need to declare a GSE when it is still not certain that an attack will occur, in order to ensure that sufficient time exists to implement pre-attack conservative operations.

As with COs that power companies adopt when they are within a hurricane's cone of uncertainty, it will be especially helpful to develop pre-attack emergency orders that will not disrupt day-to-day electric service. If the Secretary issues such orders for BPS entities to adopt COs and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented them – but only if those orders also enable entities to recover the costs of doing so. Section IV of this study examines possible “no regrets” emergency orders for conservative operations. Many of them could order COs similar to those developed for natural hazards. For example, pre-attack EOs might order BPS entities to increase generation reserves and/or re-dispatch resources out of least cost operations, and reimburse those entities for the costs they incur.

Other orders might be threat-specific: i.e., to intensify scrutiny of OT networks for malware. Power companies could implement all such no regrets EOs without cutting off power to customers or creating grid instabilities. DOE and its industry partners must consider the development of such options as a special priority for follow-on engineering and operational analysis. Appendix B contains a preliminary list of options for conservative operations which builds on current utility conservative operations procedures, and adds additional, adversary-specific options.

## **2. Putting Additional “Arrows in the Quiver:” Possible EOs for Extraordinary Circumstances**

Industry and government partners should also develop emergency orders that could offer additional benefits for protecting or restoring reliability, even at the price of disrupting normal electric service. Most such orders would be used only under extraordinary circumstances: that is, when adversaries were poised to cripple the reliable operation of the grid, and the BPS was at severe risk of instability, uncontrolled separation, or cascading failure.<sup>99</sup>

Emergency actions taken against severe natural hazards again exemplify the benefits of developing extraordinary measures for grid security emergencies. The shutdown of grid infrastructure on warning of catastrophic storm surges offers a case in point. During Superstorm Sandy, Consolidated Edison (Con Ed) faced the risk of having critical substations and underground electrical equipment inundated by the worst storm surge in nearly 200 years. If seawater hits systems that are still carrying electricity, catastrophic physical damage will result for transformers and other difficult-to-replace grid components. Consolidated Edison's team

---

<sup>99</sup> This formulation follows the definition of reliable operation in FPA, section 215, 16 U.S. Code § 824o(a)(4).

made the politically difficult decision to prevent such damage by pre-emptively cutting of power to lower Manhattan. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.<sup>100</sup> Moreover, Con Ed limited the disruptiveness of the shutdown by notifying customers hours earlier that the utility might halt service, and by already having plans in place to prioritize the restoration of service to hospitals, water-pumping stations, and other critical facilities.<sup>101</sup>

BPS entities continue to use “shutdown on warning” as an effective tool to avoid equipment damage against severe weather, and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent damage to equipment and speed restoration. Generation owners similarly chose to shut down or evacuated some generating units in the storm’s projected path.<sup>102</sup>

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and HVAC systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

Extraordinary measures designed for cyber and physical attacks may entail even greater risks and uncertainties. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an attack is likely to cause cascading failures and demonstrable harm to the U.S. economy, national security, and/or public health and safety. The potential impact of APTs on reliable grid operations may be difficult to determine until attacks are well underway. Even then, myriad factors (including many that grid operators can influence) will affect the likelihood and scope of potential cascading failures.

Nevertheless, a range of emergency orders could help BPS entities reduce the risk of cascading failures and accelerate the restoration of power if outages occur. These EOs vary in terms of when the Secretary would issue them: 1) when attacks are imminent; 2) when they are underway; and 3) when major blackouts exist, and utilities must prioritize and accelerate power restoration to prevent demonstrable, and potentially catastrophic, harm to public safety, national security, and the economy.

Emergency orders can also vary in terms of the degree of disruption they would inflict on normal electric service (and, in many instances, the specific threats they will be designed to counter). Some EOs, including no regrets orders, will have little or no disruptive impact. Others would

---

<sup>100</sup> Rich Miller, “Con Edison Shuts Off Power in Lower Manhattan,” *DataCenter Knowledge*, October 29, 2012, <http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutdown>.

<sup>101</sup> Scott DiSavino and David Sheppard, “ConEd cuts power to part of Lower Manhattan due to Sandy,” *Reuters*, October 29, 2012, <https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030>.

<sup>102</sup> North American Electric Reliability Corporation, *Hurricane Harvey Event Analysis Report*, March 2018, p. v.

have massive effects but – as in cutting off power during Sandy – would also protect grid reliability against longer term disruption and accelerate the prioritized restoration of power.

Figure 1 illustrates these different categories and examples of possible EOs that would fall within them. The leftmost column includes possible EOs that the Secretary would issue when attacks are imminent. Orders for conservative operations, especially those in the no regrets category, would fall into the lower spectrum of disruption to normal service.

**Figure 1 – Emergency Order Matrix: Examples of EO Designs**

Disruption of Normal Grid Reliability / Service	High	Pre-Planned Islanding	Prioritized Load Shedding	Movement of In-Service Transformers to Higher Priority Locations
	Low	Conservative Operations	Suspension of Wholesale Market Operations	Transportation Support for Replacement Transformers
		Protect Reliability When Attack is Imminent	Protect Reliability When Attack is Underway	Restore Service/Reliability
Grid Security Emergency Response Phase				

***a. Extraordinary Measures for Pre-Attack Protection of Grid Reliability: Islanding as a (Problematic) Example***

Pre-attack options with greater disruptive effects would populate the upper left box. Pre-planned power islanding offers an “in extremis” option that has garnered especially strong industry and government interest over the past few years. Microgrids provide the most familiar type of power island. A growing number of military installations (and a handful of hospitals and universities) have generators and other electric infrastructure on their bases, configured so that if the surrounding grid is at risk of losing power, the installations can separate themselves from the grid and operate independently as a power island.

Microgrids do not offer a “bulletproof,” all-purpose defense against imminent attacks. Cyber adversaries are sure to treat on-base electric infrastructure (including renewable generation assets and other systems) as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas-fired generators, the power they provide is only as resilient as



the gas transmission and distribution systems that supply them -- and cyber threats to natural gas systems are rapidly escalating.<sup>103</sup> Moreover, building microgrids requires extensive investment in grid infrastructure – especially if bases want to provide power not only to critical loads within their perimeters, but also for the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to traditional microgrids, power companies have also explored other means of establishing power islands when severe disruptions are imminent. Participants of GridEx, the electric industry’s premier exercise series, have extensively discussed one option that provides an especially useful basis for developing possible pre-attack emergency orders. GridEx participants note that it might be possible to pre-plan to establish large power islands by using existing grid infrastructure within their boundaries. On warning of an imminent attack or under other extraordinary circumstances, power companies would separate the power island from the surrounding grid and operate independently to serve the critical loads within it.

However, strategic islanding will only be practical if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for pre-planned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands. Moreover, standing up islands would severely disrupt day-to-day service for non-critical customers, and create instabilities for surrounding systems that could produce additional service disruptions, economic disruption, and societal unrest. Accordingly, strategic islanding might be considered a “huge regrets” emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created. Further studies will need to examine different models for pre-planned islanding, examines the design and operational challenges they would entail, and analyzes additional pre-attack options for emergency orders.

### ***b. Extraordinary Measures when Attacks are Occurring***

Emergency orders for attacks that are underway could entail similar variation in the degree to which they will disrupt normal service. The lower box in the center column of Figure 1 provides an example of a low-disruption emergency order: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate, “real time” needs or for the next day). These entities have taken extensive measures to keep these market functions separate from their operational control of the grid. Nevertheless, cyberattacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, crush the valuation of power companies on Wall Street, and magnify the damage to the U.S. economy that attacks on the grid will create.

---

<sup>103</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation’s Electricity System: Second Installment of the QER*, January 2017, p. 7-7; Paul W. Parfomak, “Pipelines: Securing the Veins of the American Economy,” *Testimony Before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*, April 19, 2016, pp. 2-3, <http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf>.

RTOs are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the Transmission Operator<sup>104</sup> for the Mid-Atlantic and other U.S. regions, has called for the development of mechanisms to permit “non-market” operations in extreme circumstances.<sup>105</sup> A number of options exist to provide for such operations. For example, if the Secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell power at a fixed price pre-determined by DOE.<sup>106</sup> Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high benefit/low disruption emergency orders examined later in this study, including orders for maximum power generation when attacks are underway, will also fall into this category.<sup>107</sup>

Utilities are already beginning to develop tools and procedures to support extraordinary operations, which DOE and industry can leverage in EO development efforts. The ESCC, for example, has led a focus on exploring how entities may operate the grid “under sub-optimal circumstances,” to ensure that these entities can anticipate, plan for, and practice using extraordinary measures to do so.<sup>108</sup> Notably, this includes the North American Transmission Forum’s “Spare Tire” program, launched in 2016, which is exploring how entities may operate the BES without primary and backup control centers.<sup>109</sup>

---

<sup>104</sup> The NERC Glossary defines Transmission Operator as: “The entity responsible for the reliability of its local transmission system, and that operates or directs the operations of the transmission Facilities.” Transmission Operator Area is defined as: “The collection of Transmission assets over which the Transmission Operator is responsible for operating.” See: “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

<sup>105</sup> PJM Interconnection, LLC, “COMMENTS AND RESPONSES OF PJM INTERCONNECTION, L.L.C.,” *In Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000), March 9, 2018, pp. 6 and 39-40.

<sup>106</sup> Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. *Ibid.*, at p. 39.

<sup>107</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see: MISO, “MISO January 17-18 Maximum Generation Event Overview” (slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018), <https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf>.

<sup>108</sup> “ESCC,” *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.

<sup>109</sup> “North American Transmission Forum External Newsletter,” *North American Transmission Forum*, January 2018, <https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf>. For more information on NATF’s Spare Tire program, see: North American Transmission Forum, *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—a Spare Tire Approach*, 2017, <http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf>.

Industry and government partners will also need to develop more disruptive EOs that can protect grid reliability in extraordinary circumstances. The top center box of Figure 1 provides a case in point: prioritized load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by shedding load – most often by implementing rotating blackouts.<sup>110</sup>

Grid operators used load shedding to protect grid reliability during the “Big Chill” that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT initiated controlled rolling blackouts during the event that affected a total of 4.4 million customers over the course of the event.<sup>111</sup> Those temporary blackouts were no doubt disruptive, especially for customers with electric heating systems. However, by reducing the risk of cascading failures, load shedding offered compelling system-wide benefits for protecting reliability.

Industry and government partners could develop emergency orders for load shedding to protect grid reliability during cyber and/or physical attacks. If adversaries are able to inflict deep, multi-region losses in generation and transmission resources, load shedding will offer an essential tool to prevent broader grid instabilities – albeit at the price of disrupting normal service to many millions of customers. NERC already requires BPS entities to have plans for load shedding.<sup>112</sup> In the EO design process, industry and government can build on that foundation to not only protect against cascading failures, but also prioritize load shedding so as to sustain service to facilities critical for national security, the economy, and public health and safety.

### ***c. Emergency Orders to Support Power Restoration***

The rightmost column in Figure 1 provides the third category for emergency orders: EOs that can help grid owners and operators restore power after widespread outages occur. In past cascading failures of the U.S. electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days or less because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators,

---

<sup>110</sup> North American Electricity Reliability Corporation, *Severe Impact Resilience: Considerations and Recommendations*, May 9, 2012, p. 11.

<sup>111</sup> FERC and NERC, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*, January 2016, p. 61.

<sup>112</sup> NERC standards currently emphasize automatic load shedding to protect grid reliability. See: NERC, *PRC-006-3 – Automatic Underfrequency Load Shedding*, effective October 1, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States); and NERC, *PRC-010-2 – Under Voltage Load Shedding*, effective April 2, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States). However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing EOs to prevent or mitigate cascading failures. See: NERC, *EOP-011-1 Emergency Operations*, effective April 1, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).

transmission lines, and other system components are designed to trip off line when instabilities occur, thereby protecting them from being damaged by power surges – and leaving them available to help rapidly re-establish the flow of power.<sup>113</sup>

However, if cyber or physical attacks destroy transformers and other critical system infrastructure, requirements to repair or replace such assets could greatly lengthen and complicate restoration operations. BPS entities already have detailed plans to restore power and, as circumstances dictate, prioritize the restoration of service to nuclear power plants and other critical customers. Industry and government should consider developing emergency orders that build on these existing plans and capabilities, and prioritize restoration for a wider array of CEI and DCEI – even if adversaries inflict unprecedented physical damage on grid components.

One option for restoration orders includes ordering utilities to operate in an N-0 operating state, unless one contingency would cause cascading failures. Currently, NERC standards require BPS entities to operate in an N-1 state: they are able to handle the most severe single contingency ('N-1').<sup>114</sup> Operators may be required to shed load to maintain the N-1 state. However, returning to an N-1 state after a major outage is likely to be a lengthy process, involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. If the Secretary were to order utilities to operate at N-0 as needed, they could do so without facing punishment for violating NERC standards. Creating such an option would provide greater operating flexibility and ensure that entities can continue to serve as much load as possible. Entities would only be required to shed load for the most severe single contingency if that single contingency would cause cascading failures or following a contingency that required load shedding to eliminate overloads or low voltage.

Restoration EOs should also account for the risk that adversaries will continue their attacks as power companies begin restoring service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to U.S. military bases and other vital facilities, and seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeted against power restoration operations can help achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply.

The Department of Defense can play a vital role in preventing such attacks. If directed by the President, United States Cyber Command (USCYBERCOM) and other DOD components would do their utmost to “shoot the archer,” and prevent the adversary’s cyber forces from launching further strikes on the grid and other U.S. targets. But re-attacks may nevertheless occur. For example, unless power companies thoroughly scrub advanced persistent threats already hidden

---

<sup>113</sup> NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, December 2010, p. 1. See also: U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 8.

<sup>114</sup> North American Electric Reliability Corporation, *BAL-002-2(i) – Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event*, Requirement R2, effective January 1, 2018.

their networks, those APTs may launch repeated re-attacks against the grid and create recurring outages.<sup>115</sup> Physical attacks to disrupt restoration operations, including against replacement transformers being moved to critical substations, would create additional challenges.<sup>116</sup>

As with EOs for imminent and ongoing attacks, emergency orders to accelerate power restoration will differ in their disruptiveness to normal grid operation. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks and barges) from where power companies store them to where they are needed as replacements.<sup>117</sup> The Secretary has no authority under the Federal Power Act to issue orders to transportation sector assets. However, in collaboration with the Department of Transportation, rail and other asset owners, and SLTT transportation agencies, DOE and the private sector could pre-plan to waive transportation regulations, inspection requirements, and other potential impediments on a nationwide basis. Such plans could also be structured to help protect transportation operations against active shooters or other attacks.

EOs could also be created for *in extremis* restoration operations that would more sharply depart from existing industry plans and procedures. As the starting point for that development process, power companies and their government partners might assume that attacks will not be “one and done,” but instead be part of a sustained campaign in which adversaries will single out restoration operations for disruption. An example of *in extremis* orders: if adversaries managed to damage or destroy an extraordinarily large number of transformers, the Secretary might order that surviving, in-service transformers in the same voltage class be removed from their substation and transported to serve vital national security facilities in the National Capitol Region or other areas. Such orders could create severe disruptions in existing service. However, the benefits might be greater still for helping the United States defeat its adversary.

### **3. Next Steps in the EO Development Process**

Potential emergency orders differ not only in terms of the phases of an attack in which they would be most useful, and in their mix of benefits and disruptive impact on normal grid operations, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create – especially those that fall into the “no regrets” category. As noted above, utilities frequently use COs to help protect grid reliability in severe weather events, and a growing number of companies are already building on that foundation to draft equivalent COs against cyber and physical threats.<sup>118</sup> Emergency orders based on those initiatives constitute “low hanging fruit;” creating such orders offers an immediate opportunity

---

<sup>115</sup> Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee: Part I – Incident Response*, June 2016, p. 7.

<sup>116</sup> The GridEx exercise series accounts for physical attacks that disrupt restoration operations. See: NERC, *Grid Security Exercise: GridEx III Report*, March 2016.

<sup>117</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, pp. 12-13, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>118</sup> PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 54.



for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging EO initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are underway, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. The next step to do so is to examine how emergency orders can be framed to reflect and achieve specific U.S. security priorities and meet the other development requirements that they will entail.

#### **IV. ADDITIONAL EMERGENCY ORDER DESIGN PARAMETERS AND SUPPORTING INITIATIVES**

The U.S. *National Security Strategy* provides crucial guidance on how emergency orders can help deter attacks on the grid and other U.S. targets, and how those orders can help the United States defeat adversaries if deterrence fails. However, DOE and BPS entities will also need to overcome the immense communications challenges that the use of emergency orders will entail, including requirements to explain to the U.S. public why extraordinary measures are being employed and what they should expect if attacks continue. Incorporating provisions for regulatory waivers and cost recovery in the design of template emergency orders will offer compelling advantages as well.

##### **A. DETERRING AND DEFEATING U.S. ADVERSARIES**

Adversaries will strike the U.S. grid not merely to cause blackouts, but as a means to help them achieve their broader political, economic, and military objectives against the United States. Government and industry partners should design emergency orders to help prevent attackers from accomplishing their objectives, and – ideally – help deter them from attacking at all.

The U.S. *National Security Strategy* offers an overarching framework to guide such design efforts. The *Strategy* emphasizes that cyber threats to U.S. critical infrastructure are becoming increasingly severe, and notes that cyber weapons “enable adversaries to attempt strategic attacks against the United States – without resorting to nuclear weapons – in ways that could cripple our economy and our ability to deploy our military forces.”<sup>119</sup> To counter these threats, the *Strategy* identifies two essential priorities, both of which emergency orders can be designed to support:

- Deter adversaries from attacking by convincing them they will suffer “swift and costly consequences” and be defeated if they strike the grid or other U.S. targets;<sup>120</sup>
- Strengthen infrastructure resilience to make adversaries doubt that “they can achieve their objectives” if they do attack (i.e. deterrence by denial).<sup>121</sup>

---

<sup>119</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 27.

<sup>120</sup> *Ibid.*, at p. 28.

<sup>121</sup> *Ibid.*, at p. 13.

## **1. Deterrence through Threats of Punishment and Defeat: Implications for Emergency Order Design**

One important way that emergency orders can strengthen deterrence is by helping convince adversaries that the United States will be able to effectively respond to attacks and impose consequences that those adversaries would consider unacceptable. A relatively small number of U.S. military bases are responsible for conducting such response operations. The U.S. Defense Science Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of U.S. strike systems (cyber, nuclear, and non-nuclear) and supporting infrastructure to ensure “that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyberattacks.”<sup>122</sup> Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should and immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which U.S. strike systems rely and ensure that they have reliable power for however long a conflict might continue.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The *Strategy* emphasizes that “We must convince adversaries that we can and will defeat them – not just punish them if they attack the United States.”<sup>123</sup> As noted in Section II, adversaries are most likely to attack the grid in the context of an intense regional confrontation with the United States and its allies in the South China Sea, the Baltics, or some other crisis abroad. A vast array of U.S. Defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy and sustain U.S. power projection forces for regional contingencies. Ensuring the availability of resilient power for these essential facilities and functions will require the development of emergency orders to serve a greatly expanded set of customers than for U.S. strike systems alone, and encompass a much larger array of DCEI owners and operators.

Emergency orders and implementation plans will need to account for a further challenge: the risk that adversaries will selectively target defense critical electric infrastructure and prioritize its disruption through especially sophisticated cyber and physical attacks. The Department of Defense (DOD) *Mission Assurance Strategy* (2012) emphasizes the growing risk that adversaries will seek to degrade U.S. military capabilities by attacking the infrastructure on which DOD depends. In particular, “Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting critical Defense and supporting civilian capabilities and assets,” including the U.S. power grid.<sup>124</sup>

---

<sup>122</sup> James N. Miller and James R. Gosler, “Memorandum for the Chairman, Defense Science Board” (preamble), *Task Force on Cyber Deterrence*, February 28, 2017. See also: Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, pp. 3, 6-7, 11-12, and 17-18.

<sup>123</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 28.

<sup>124</sup> Department of Defense, *Mission Assurance Strategy*, April 2012, p. 1, [http://policy.defense.gov/Portals/11/Documents/MA\\_Strategy\\_Final\\_7May12.pdf](http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf).

Electric companies and Defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds to serve Defense installations provides a valuable means of strengthening resilience.<sup>125</sup> Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.<sup>126</sup> And, as briefly discussed in Section II, utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as “power islands” independent of the surrounding grid.<sup>127</sup>

While valuable, these initiatives do not eliminate the need to develop Defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases. Emergency generators will break down in long duration outages, and resupplying them with fuel will become increasingly difficult at installations that lack massive storage tanks. Large-scale microgrids for islanded operations can provide more resilient power; DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for warfighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, ranging from the water utilities and other “outside the fence” infrastructure that support base operations, to the intermodal transportation systems that help deploy and sustain U.S. forces abroad.

Emergency orders can help support deterrence and power projection far more quickly and with less infrastructure investment. Over the past year, the Department of Defense has been collaborating with power companies and DOE to develop new emergency measures to protect the resilience of electric service to military bases by prioritizing the flow of power to bases when generation capacity falls short of total load, and through other emergency operations. BPS entities are also launching initiatives with DOD and DOE to ensure that power to Defense installations can be restored far more rapidly than is possible today if adversaries create wide-area blackouts.<sup>128</sup>

---

<sup>125</sup> Department of Defense (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment), *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*, July 2017, p. 39, <https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf>.

<sup>126</sup> *Ibid.*, at 40.

<sup>127</sup> *Ibid.* at 39. See also: Lincoln Laboratory, *Microgrid Study: Energy Security for DoD Installations* (Technical Report 1164), June 2012, <https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf>; and Pew Charitable Trusts, *Power Begins at Home: Assured Energy for U.S. Military Bases*, January 12, 2017, pp. 13-15. A number of “islandable” microgrid projects are underway at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See: Michael McGhee, “EEI Executive Advisory Committee,” (slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017), p. 4, [http://www.asaie.army.mil/Public/ES/oei/docs/EEI\\_Exec-Committee.pdf](http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf); and Cheryl Kaften, “DoD Tests Energy Continuity with ‘Islanded’ Microgrid,” *Energy Manager Today*, April 5, 2017, <https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/>.

<sup>128</sup> “Rapid Attack Detection, Isolation and Characterization Systems (RADICS),” *Defense Advanced Research Projects Agency*, n.d.a., <https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems>.

These initiatives provide an increasingly robust foundation for developing emergency orders to reinforce U.S. deterrence and power projection capabilities. For protection against imminent attacks, it may be possible for power companies to develop plans for conservative operations that are specially targeted to protect the defense critical electric infrastructure in their service areas. Pre-planned islanding could provide unique benefits for military bases and supporting systems (though only if power companies can overcome the immense technical and operational impediments such islanding entails). The development of EOs and company-specific implementation plans for prioritized load shedding, in extremis restoration support, and other potential orders also offer additional opportunities to build on industry-government collaboration already underway for post-attack emergency operations.

The prerequisite for these development efforts will be for the Secretary to identify which military bases and supporting assets are most critical to protect. Section 215A of the Federal Power Act provides a starting point to do so. The Act requires the Secretary of Energy, in consultation with other Federal agencies and grid owners and operators, to identify and designate “critical Defense facilities” in the 48 contiguous states and the District of Columbia that are “1) critical to the defense of the United States; and 2) vulnerable to a disruption of electric energy provided to such facility by an external provider.”<sup>129</sup> Congress also created a definition of *Defense Critical Electric Infrastructure* (DCEI) to help guide implementation of that requirement. DCEI constitutes “any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]” as a critical Defense facility, “but is not owned or operated by the owner or operator of such facility.”<sup>130</sup>

The Department of Energy is already working with the Department of Defense to identify and strengthen the resilience of power flows to critical Defense facilities. DOE is also already working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate infrastructure identified as DCEI. Fortunately, DOD already has a well-established, continuously-updated list of Defense Critical Infrastructure (including military bases and other assets) to help provide input to DOE.<sup>131</sup> A wide variety of factors contribute to determining the criticality of a particular military base or other Defense asset. However, for designing emergency orders that help achieve the deterrence and defense priorities of the *National Security Strategy*, priorities for protecting and restoring service fall into three categories. Figure 2 depicts these categories as a set of concentric circles.

## Figure 2 – Categories for Protecting Defense Critical Electric Infrastructure

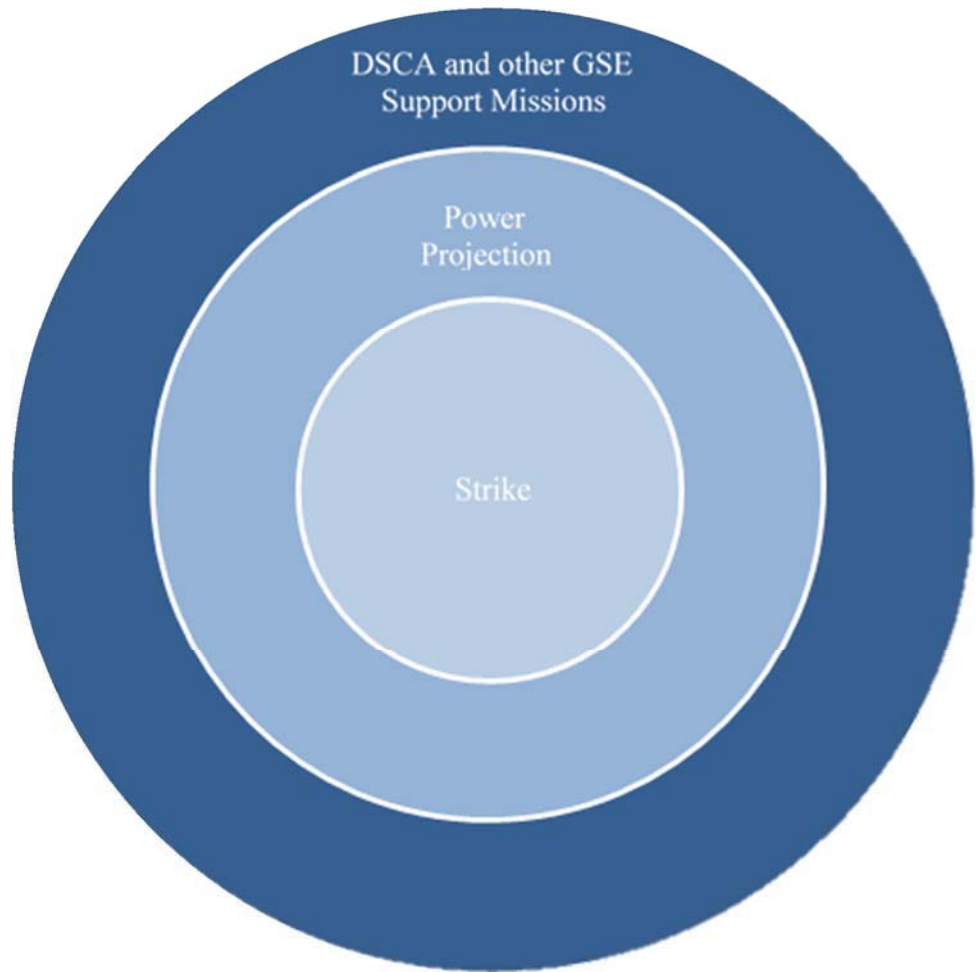
---

<sup>129</sup> 16 U.S.C. § 824o–1, Section (c), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>130</sup> 16 U.S.C. § 824o–1, Section (a)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>131</sup> See: Department of Defense, *Department of Defense Manual 3020.45: Defense Critical Infrastructure Program (DCIP): Execution Timeline*, last updated May 23, 2017, <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>; and Department of Defense, *Department of Defense Directive 3020.40: Mission Assurance (MA)*, November 29, 2016, [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).

At the innermost core lies those installations and supporting infrastructure that are essential for inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital; protecting the reliability of the DCEI on which they depend is crucial and should be the top priority for developing emergency orders and company-specific implementation plans.



The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining them abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the U.S. grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. The Department of Defense is in the process of identifying the specific facilities and supporting infrastructure that is required to help execute Operational Plans (OPLANS) around the globe.<sup>132</sup> DOD also has well-established criteria and assessment methods to prioritize these supporting assets for risk-mitigation.<sup>133</sup> These tools should be used to identify the broader set of defense critical electric infrastructure needed for deterrence, and to help power companies pre-plan to support critical assets within their service footprints.

<sup>132</sup> Department of Defense, *Department of Defense Directive 3020.40: Mission Assurance (MA)*, November 29, 2016, [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).

<sup>133</sup> Department of Defense, *Department of Defense Manual 3020.45: Defense Critical Infrastructure Program (DCIP): Execution Timeline*, last updated May 23, 2017, <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>



The third circle includes the still larger array of Defense installations, including National Guard bases, which would be essential for providing Defense Support to Civil Authorities (DSCA) if disruptions of the grid jeopardize public health and safety. In Hurricane Maria (2017), superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and providing other assistance. Protecting or rapidly restoring the reliability of the DCEI that supports these DSCA functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public. Ultimately, however, countering such adversary efforts will require protecting grid service to the still broader array of hospitals, water systems, and other civilian assets served by critical electric infrastructure.

## **2. Deterrence by Denial: Protecting Critical Electric Infrastructure**

Emergency orders can also strengthen deterrence through a very different means. In addition to deterring adversaries by threatening to inflict unacceptable costs if they attack, and being able to defeat them abroad if war occurs, the United States can also discourage attacks by making adversaries doubt that those attacks can inflict major disruptions on the grid. The *National Security Strategy* notes that “A stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.”<sup>134</sup> Bolstering such “deterrence by denial” constitutes a prime goal for developing emergency orders, as well as a source of challenging design requirements.

A special advantage of deterrence by denial is that it does not rely on attack attribution to discourage adversaries from striking the grid. Threats to impose unacceptable costs on attackers will only work if adversaries believe that the United States will be able to identify them as the perpetrators. To evade punishment, attackers are likely to take extraordinary technical measures to complicate or defeat such attribution. The Federal Bureau of Investigation and other Federal agencies need to continue strengthening their attribution capabilities accordingly.<sup>135</sup> FPA information sharing mechanisms can support such improvements by helping speed and secure the delivery of malware samples and other threat signature information between utilities and government agencies.<sup>136</sup>

Nevertheless, despite these efforts, sophisticated adversaries may still doubt whether the United States will be able to identify them as the attacker. Emergency orders that bolster grid resilience can support a different means to deter these adversaries. By helping power companies sustain service to essential customers, emergency orders can heighten adversary doubts as to whether

---

<sup>134</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 13.

<sup>135</sup> Scott S. Smith, “Roles and Responsibilities for Defending the Nation from Cyber Attack,” *Testimony Before the Senate Armed Services Committee*, October 19, 2017. See also: Lily Hay Newman, “Hacker Lexicon: What is the Attribution Problem?,” *WIRED*, December 24, 2016, <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.

<sup>136</sup> See: 16 U.S.C. § 824o–1, Section (d), <https://www.law.cornell.edu/uscode/text/16/824o-1>. Later sections of this study provide a more detailed assessment of provisions for improved information sharing.

attacks will be effective and reduce the expected benefits of striking the grid regardless of U.S. attribution capabilities.

Orders that contribute to deterrence by denial will also be useful against adversaries who do not care that the United States will punish them for attacks on U.S. critical infrastructure. For threats of cost imposition to work, the United States must be able to identify and destroy things that foreign leaders would find intolerable to lose.<sup>137</sup> However, it will be very difficult to target anything that leaders of the Islamic State would find so precious.<sup>138</sup> Deterring cyberattacks through threats of punishment could also be difficult against leaders such as Kim Jong Un.<sup>139</sup> Emergency orders can provide an alternative means to discourage these adversaries from attacking the grid by reinforcing their doubts that they can achieve the disruptive effects they seek.

Finally, emergency orders and the improvements in grid resilience they provide could help U.S. leaders prevail in future confrontations. In regional conflicts that have not yet escalated to full-scale cyberattacks against the United States, U.S. leaders may wish to launch carefully-selected strikes (via cyber or conventional means) against adversaries to encourage them to de-escalate and negotiate for peace. Those leaders may be reluctant to employ strike options if they believe adversaries could cripple the U.S. grid in response. By strengthening the confidence of the President and his advisers that the grid can survive attack(s), and sustain service to essential facilities and functions, emergency orders can help widen the range of options available to the President to resolve future conflicts.<sup>140</sup>

Emergency orders will need to meet stringent design requirements to achieve these goals. To strengthen deterrence by denial, and – if deterrence fails – help ensure that the United States will prevail in a conflict, a large and exceptionally diverse set of customers will need resilient power.

---

<sup>137</sup> Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 3.

<sup>138</sup> Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 4; Brian Michael Jenkins, “Countering al-Qaeda: The Next Phase in the War,” *RAND*, September 8, 2002, <https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html>.

<sup>139</sup> Egle Murauskaite, “North Korea’s Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment,” *38 North (US-Korea Institute at Johns Hopkins SAIS)*, September 12, 2014, <http://www.38north.org/2014/09/emurauskaite091214/>. In contrast, James Andrew Lewis argues that “the primary objective of the North Korean state and the Kim family is regime survival” and they will be loath to put that survival at risk by striking the U.S. grid and other critical infrastructure. James A. Lewis, “North Korea and Cyber Catastrophe—Don’t Hold Your Breath,” *38 North (US-Korea Institute at Johns Hopkins SAIS)*, January 12, 2018, <http://www.38north.org/2018/01/jalewis011218/>. On the broader challenges of tailoring threats of punishment to deter specific nations and foreign leaders, see Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 12.

<sup>140</sup> Even if the United States greatly strengthens grid resilience, the use of cyber weapons in future conflicts will be fraught with risks of rapid (and perhaps unintended) escalation. Jim Miller and Richard Fontaine argue that structural incentives exist for rapid escalation in cyberspace, and that adversaries will have incentives to employ cyber capability “in large doses early in a major conflict to gain coercive and military advantage – and to attempt to prevent the other side from gaining such an advantage.” Miller and Fontaine, *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies are Reshaping Pathways to Crisis and Conflict*, September 2017, p.16.

See also: Jason Healy, “The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities,” *Columbia University*, June 2016, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2836206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206).

Only a limited set of military bases and supporting civilian assets are critical to the defense of the United States. However, adversaries may seek to not only disrupt U.S. Defense capabilities, but also jeopardize societal continuity by crippling electric service to regional hospitals, major financial institutions, and other facilities essential to the U.S. economy and public health and safety.

### **3. Building a “Section 9+ List:” Prioritizing Infrastructure for Sustainment and Restoration**

The Federal Power Act emphasizes the need to protect and restore CEI which, if destroyed or incapacitated, would “negatively affect” national security, the U.S. economy, and public health or safety. But such effects could result from the loss of power to many thousands of hospitals, water utilities, communications systems, and other assets spread across all 16 critical infrastructure sectors. Industry and government do not have the operational resources required to sustain and rapidly restore all critical infrastructure that may be impacted by a large-scale attack.

DOE and its private sector partners will therefore need to pre-identify a far more specific and stringently-prioritized list of critical assets and supporting CEI to protect. To develop template emergency orders and contingency plans to implement them, industry and government will need to determine which specific customers (and the critical electric infrastructure that serves them) are the most critical recipients of prioritized power flows if normal service breaks down.

Executive Order 13636 (February 2013) provides the best methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the Secretary of Homeland Security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.”<sup>141</sup> That standard – catastrophic damage – provides a basis to identify the highest priority assets and associated CEI for protection by emergency orders in GSEs. Over time, orders and contingency plans could gradually encompass less critical facilities and grid infrastructure.

Of course, the Section 9 methodology and subsequent list were never intended to support the implementation of Section 215A of the FPA. As a result, the Section 9 methodology falls short of meeting all the requirements for supporting emergency order design. This methodology, for example, is designed specifically for cybersecurity incidents. Meanwhile, the FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on critical grid assets. EO 13636’s Section 9 requirements also create a “corporate” level list that is not broken down to the key priorities within the corporation (i.e., facilities, systems, and nodes). Identifying the most critical assets and facilities as priorities in GSEs will require a more fine-grained analysis which considers the increasingly complex interdependencies of U.S. critical infrastructure.

---

<sup>141</sup> Executive Order 13636 – *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

Despite these shortfalls, DHS' Executive Order 13636 methodology can provide a valuable starting point for identifying the most vital CEI and supporting assets. DOE and its industry partners should leverage that methodology to create a "Section 9+" list, tailored to fulfill FPA emergency order requirements. Other government efforts to prioritize critical infrastructure, could also make valuable contributions to the list and overall prioritization effort.<sup>142</sup> However, further impediments exist to ensuring that such a list will be effective.

The Section 9 methodology, for example, lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the Federal government tells grid owners and operators if they are on the Section 9 list, they are rarely informed about the Section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data. The Federal government will therefore face inherent problems in building a list of the most critical infrastructure assets and components nationwide.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that individual pharmaceutical distributors, suppliers of water system treatment chemicals, and other companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations in one industry can produce unintended and unforeseen effects on overall system resilience. Yet, companies have powerful incentives to resist sharing such business-sensitive, proprietary information. Public sector leaders will therefore have to strengthen their industry counterparts' confidence that government agencies would not use this data for regulatory compliance, antitrust, or other purposes not explicitly approved through industry-government dialog.

---

<sup>142</sup> There are numerous examples. DHS' National Critical Infrastructure Prioritization Program (NCIPP) aims to identify "nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance." See: DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, p. 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on "lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity." *Ibid.*, at p. 30. Despite its focus on terrorist threats, HSPD-7 also requires the Secretary of Homeland Security to identify and prioritize systems and assets, which, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. DHS, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, <https://www.dhs.gov/homeland-security-presidential-directive-7>. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the "loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States" and lower jurisdictions. The national level priorities on this list could also be helpful. Section (a)(2), 6 U.S.C. § 1241 – *National asset database*, <https://www.law.cornell.edu/uscode/text/6/1241>.

Securing and containing the distribution of this classified data will also be a crucial consideration. The Section 9+ list or equivalent prioritization efforts, if obtained by adversaries, would serve as an instructive guide on how to maximize the devastation of U.S. critical infrastructure and provide a strategic roadmap for attack. To ensure the Section 9+ list's utility in enabling planning and order design, however, essential efforts to protect this data must be complemented by an improved scheme for providing the data to appropriate individuals (with the required security clearance).

## **B. COMMUNICATIONS REQUIREMENTS FOR ISSUING AND EMPLOYING EMERGENCY ORDERS**

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phone and other normal means of communication fail. Under the Electricity Subsector Coordinating Council (ESCC), they have also built an extensive set of “playbooks” to help companies decide what to tell customers about the incident, and to create “unity of messaging” between government officials and industry representatives on estimated times of restoration (ETRs) and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. In anticipation of attacks causing grid security emergencies, these partners have the opportunity to focus on three specific challenges: 1) maintaining survivable communications systems for issuing and sustaining the implementation of emergency orders; 2) preventing adversaries from gaining access to sensitive emergency orders and classified information; and 3) determining what to say to the U.S. public about the attack, potentially including strategies for countering adversary efforts to intensify public panic and incite disorder.

Requirements for survivable and secure communications will be widely shared across many types of grid security emergencies and template EOs. The section that follows offers recommendations to help meet these common needs. In contrast, for informing the U.S. public as to why the Secretary has issued emergency orders and what customers should expect, “no regrets” conservative operations will generate only minor challenges compared to prioritized load shedding and other orders that disrupt normal service. Pre-planning for such “strategic messaging” will be vital to counter the political leverage that adversaries will seek by attacking the grid and should be an integral part of the emergency order design process.

### **1. Communications Requirements in Grid Security Emergencies**

As with the phases of grid security emergency declarations (starting when attacks are imminent), the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Pre-attack



consultations constitute the initial stage. The Federal Power Act specifies that before the Secretary issues EOs, DOE will consult with power companies and other BPS stakeholders “to the extent practicable...regarding implementation of such emergency measures.”<sup>143</sup> This study also recommends that Federal officials consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The Final Rule on *Grid Security Emergency Orders: Procedures for Issuance* clarifies how DOE’s Office of Electricity Delivery and Energy Reliability (OE) will consult on EOs. The GSE Rule specifies that, if practicable, the Electricity Information Sharing and Analysis Center (E-ISAC) is one of the organizations with which the Secretary will consult. Such consultations will be especially useful for sharing data (including classified data) on attacks that are imminent or underway. The GSE Rule also notes that OE will consult with the Electricity Subsector Coordinating Council (ESCC). The ESCC will provide an especially valuable source of industry perspectives on GSE declarations and EOs because the Council represents all components of the electricity subsector and has extensive experience in coordinating industry incident response operations. In addition, the GSE Rule states that “efforts will be made” to consult with NERC, regional entities such as Regional Transmission Operators, “owners, users or operators” of CEI and DCEI, appropriate Federal and state agencies, and other grid reliability stakeholders.<sup>144</sup>

Issuing emergency orders constitutes the second stage. The GSE Rule states that DOE will “communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances.”<sup>145</sup> However, DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.<sup>146</sup> Doing so will be much more efficient and effective than creating a separate, unfamiliar system for communicating emergency orders. Using established communication systems also has the added benefit of pre-existing legitimacy, which can help DOE and utilities avoid potential questions over authentication and possible adversary attempts to spoof EOs. Industry should provide recommendations to DOE on how best to communicate orders to BPS entities to ensure they will be effectively implemented.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders and monitor their compliance with those EOs. Attacks on the grid are unlikely to be “one and done.” As adversaries continue to try to create grid instabilities, and power companies respond with emergency operations to prevent cascading failures, maintain service to critical facilities, and restore power while under attack, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional EOs and response activities – potentially on a nationwide basis. Reliability Coordinators (RCs) will be a critical touchpoint between DOE and individual

---

<sup>143</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1774

<sup>144</sup> *Ibid.*, at p. 1181.

<sup>145</sup> *Ibid.*

<sup>146</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177

BPS entities. RCs can serve as a focal point between DOE and other government leaders and the BPS entities which are in their purview.

Sustained communications will also be necessary to meet an additional requirement of the Federal Power Act: enforcement of emergency orders. The GSE Rule specifies that “Beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order.”<sup>147</sup> Moreover, “in accordance with available enforcement authorities, the Secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order.”<sup>148</sup>

## **2. Survivability of Communications**

Adversaries will have compelling incentives to combine attacks on the grid with strikes against U.S. communications systems. The 2015 attack on Ukraine’s electric system illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone system; the latter attack prevented customers from reporting outages and disrupted the ability of grid operators to focus on restoration operations accordingly.<sup>149</sup> In turn, if adversaries can lengthen power outages by disrupting communications systems essential for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually-reinforcing disruptions in both sectors.

We should assume that adversaries will attack to maximize these failures, especially since they would already be facing the risk of U.S. response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry-government coordination in grid security emergencies.

The likelihood of such combined attacks will intensify as DOE and its partners move through the sequential communications stages of grid security emergencies. Risks will be lowest in the consultation phase. That is fortunate. Under the ESCC, the electric industry has created extensive mechanisms to coordinate response operations by multiple power companies and coordinate mutual assistance operations with DOE and other government agencies. Consultations on possible emergency orders will leverage that existing ESCC system.

To date, however, ESCC consultations on response operations have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to

---

<sup>147</sup> *Ibid.*, at p. 1182.

<sup>148</sup> *Ibid.*

<sup>149</sup> “Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure,” *ICS-CERT*, February 25, 2016, <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.

distributed denial of service (DDoS) attacks and a range of other increasingly severe threats,<sup>150</sup> as well as the communication sector's reliance on grid-provided electricity (especially in long duration outages that put emergency power assets at risk).

The GSE Rule notes the Department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include "essential actions" to protect bulk power system reliability which require recipients to respond as defined in the alert.<sup>151</sup> DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across the bulk power system. NERC already distributes alerts broadly to users, owners, and operators of the bulk power system in North America. Hence, for issuing emergency orders, the alert system provides DOE with an opportunity for "one stop shopping." The Secretary could issue an order to NERC for distribution to both regional operating organizations (RTOs, ISOs, Reliability Coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is e-mail-based.<sup>152</sup> As a result, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also only includes those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for sustaining power to critical facilities and for implementing emergency orders for prioritized load shedding and other actions.

Industry and government partners should consider additional measures to bolster that alert system or create fallback options for the Secretary to issue orders when attacks are underway. Satellite phones may provide an especially prominent option. Those phones are widely deployed both by BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies. General William Shelton (USAF-Ret.) who directed the U.S. Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these

---

<sup>150</sup> Russ Banham, "DDoS Attacks Evolve To Conscript Devices Onto The IoT," *Forbes*, February 4, 2018, <https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#4b5a43a86aaa>.

<sup>151</sup> "About Alerts," *NERC*, n.d.a., <http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx>.

<sup>152</sup> *Ibid.*

counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community.”<sup>153</sup>

The most difficult challenges for communications in a GSE would emerge as BPS entities implement emergency orders, and power companies coordinate with DOE on emergency operations and respond to follow-on strikes. Communications systems are likely to be under comprehensive attack during this stage. To prepare against that risk, power companies are ramping up their investments in emergency communications systems that are hardened against cyber and physical attacks, and can be used to sustain critical grid functions even if satellite phones fail.<sup>154</sup> Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are underway in building dark fiber or other survivable links between BPS entities – much less between those entities and DOE. The National Infrastructure Advisory Council study on *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish “separate, secure communications networks specifically designated for the most critical cyber networks, including ‘dark fiber’ networks for critical control system traffic and reserved spectrum for backup communications during emergencies.”<sup>155</sup>

The study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities “can communicate with utility crews working in the field to manually restore power” and conduct other post-attack operations.<sup>156</sup> Survivable communications systems will also need to enable the same multi-company decision-making and coordination with government that the ESCC already employs for hurricanes and other natural disasters. The development and deployment of such systems must be part of broader effort to prepare for grid security emergencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when they are needed most.

### **3. Securing Sensitive Emergency Orders and Classified Information**

Certain types of emergency orders may be vulnerable to countermeasures if adversaries gain access to them. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as

---

<sup>153</sup> General William L. Shelton, USAF (Ret), “Threats to Space Assets and Implications for Homeland Security,” *Written Testimony Before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*, March 29, 2017, p. 3, <http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf>.

<sup>154</sup> Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC), *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans – Further Joint Study: Planning Restoration Absent SCADA or EMS (PRASE)*, June 2017, p. 15.

<sup>155</sup> NIAC, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, August 2017, p. 7. <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>

<sup>156</sup> *Ibid.*

possible, lest those operations create incentives for adversaries to strike before their APTs were disabled. When attacks are underway, it could be useful to deny adversaries the knowledge of where and how BPS entities were prioritizing the flow of power to key military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The Federal Power Act and subsequent GSE Rule provide for the sharing of classified information in grid security emergencies. The GSE Rule specifies that:

To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.<sup>157</sup>

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program (CRISP) already have mechanisms and protocols for sharing and securing classified threat data with BPS entities cleared for access to that data.<sup>158</sup> Industry and government partners should consider building on those mechanisms to support the issuance of classified EOs. However, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Moreover, for utilities with cleared personnel on their staffs, an even smaller number possess the Sensitive Compartmented Information Facilities (SCIFs) or other infrastructure and government approvals to store classified information. To address those limitations, the GSE Rule clarifies that the Secretary may declassify information critical to the emergency response.<sup>159</sup> But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of Combatant Commander operational plans; when EOs may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

#### **4. Communicating with the American People**

Adversaries may attack the grid not only to disrupt national defense and the economy, but also to gain political leverage over U.S. leaders by inciting public panic and disorder. A presidential declaration that the grid faced imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks

---

<sup>157</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1182.

<sup>158</sup> “Energy Sector Cybersecurity Preparedness,” *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

<sup>159</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1778.



and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the U.S. public.

Pre-planning for public messaging to accompany GSE declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Providing for unity of messaging with governors and other elected officials on estimated times of restoration (ETRs) can present significant challenges in such events. However, those difficulties will be dwarfed by the problems that cyberattacks will create. GridEx IV (November 2017) highlighted a number of such problems. They include:

- Adversary use of information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety;
- Disruption of normal means of communication on which the public will rely for information about the event; and
- Inherent difficulties of estimating ETRs when adversaries employ advanced persistent threats that enable repeated re-attacks and disruptions in grid service until eradicated from BPS networks.

The ESCC and its members are developing playbooks to help meet these challenges, and to support public messaging in the event of cyber or physical attacks against the grid.<sup>160</sup> Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that Presidential GSE declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Pre-planning for message coordination with Canada and Mexico could also be helpful and might leverage the Federal Power Act's provisions for such multi-national consultations concerning the issuance of emergency orders.<sup>161</sup>

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. Some orders that will be valuable for protecting grid reliability, including EOs for prioritized load shedding, could cut off electricity to many thousands of customers in order to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by pre-planned communications playbooks to address customer concerns.

### **C. THE DEEPER VALUE PROPOSITION FOR EMERGENCY ORDERS: ENFORCEMENT, WAIVERS, AND COST RECOVERY**

---

<sup>160</sup> "ESCC," *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.

<sup>161</sup> 16 U.S.C. § 824o-1, Section (b)(3), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

Conservative operations offer an attractive starting point to develop pre-attack emergency orders because so many power companies already have extensive, frequently-used COs in place. For post-attack orders, NERC reliability standards provide a similarly well-established foundation for load shedding and other extraordinary measures. Emergency orders to accelerate power restoration can draw on a mutual assistance system that utilities have been refining for decades. These existing means of protecting and restoring grid reliability are so effective that they beg the question: how can emergency orders add value for defending the bulk power system and provide benefits beyond those that industry-based measures already offer?

EOs provide a unique means to ensure that BPS entities' emergency plans directly support U.S. deterrence goals and other national security priorities. As DOE and its partners identify critical electric infrastructure and defense critical electric infrastructure, and share that data with BPS entities, the electric industry will also be better positioned to develop utility-specific plans to sustain or restore service to vital facilities.

The development of template emergency orders will provide other benefits as well. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting COs to meet the specialized challenges posed by cyber and physical threats.<sup>162</sup> The industry-government process to develop emergency orders will provide a basis to share emerging best practices and embed them in utility plans for grid security emergencies.

The EO development process will also help protect grid reliability against nationwide threats. While hurricanes and other familiar natural hazards affect only limited geographic areas, adversaries may use cyber weapons to simultaneously attack all three interconnections in the United States. Communicating EOs in real time to utilities across the country may pose a challenge. DOE and the electricity subsector already have mechanisms in place to alert utilities when adversaries are implanting malware on critical systems, including the Cybersecurity Risk Information Sharing Program (CRISP) and other E-ISAC notification procedures and portals.<sup>163</sup> This includes the E-ISAC's new "Critical Broadcast Program," which is intended to operationalize their information sharing capabilities.<sup>164</sup> The Federal Bureau of Investigation (FBI) and DHS also issue alerts to the energy sector, as in the case of Nuclear 17 (June 2017)

---

<sup>162</sup> See, for example, PJM, *PJM Manual 13: Emergency Operations* Revision 64, June 1, 2017, p. 73; Todd Lucas (Southern Company), "Conservative Operations," (presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, Colorado, September 18-19, 2013), <http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf>; and SERC Reliability Corporation, *Conservative Operations Guidelines* Guide-800-101, May 20, 2015, [https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines\\_rev-0-\(05-20-15\).pdf?sfvrsn=2](https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2).

<sup>163</sup> "Energy Sector Cybersecurity Preparedness," *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>; "Electricity ISAC," *NERC*, n.d.a., <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>164</sup> The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See: Bill Lawrence, Charlotte de Seibert, and Philip Daigle, "E-ISAC Update," (presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, Florida, March 6-7, 2018), <https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf>.

and Crash Override.<sup>165</sup> However, when the President determines that there is an imminent danger of attacks on the grid, the Secretary will need a speedy and reliable system to trigger the implementation of conservative operations (including, potentially, specialized malware search and eradication measures) on a nationwide basis. Leveraging existing alert systems to support the issuance and execution of EOs will expedite preparedness for GSEs. It will also be essential to assess how adversaries might seek to disrupt the use of these existing systems, and supplement them as needed.

Developing EOs will facilitate nationwide exercises as well. NERC already requires BPS entities to exercise their individual emergency plans. In the GridEx exercise series, over 100 utilities across the United States and Canada exercise their plans against combined cyber-physical attacks and have an opportunity to share lessons learned. Building template emergency orders and utility-specific implementation plans would provide an even stronger basis for coordinated, multi-entity exercises against a notional threat, including the issuance and execution of emergency orders for all three phases of grid security emergencies.

Beyond these preparedness benefits, specific components of the Federal Power Act and GSE Rule create additional opportunities for added value – particularly if industry and government partners plan in advance for their mutual benefit.

## **1. Enforcement and Political “Top Cover”**

The GSE Rule specifies that “in accordance with available enforcement authorities, the Secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that order.”<sup>166</sup> The prospect that BPS entities will be punished for refusing to comply with poorly-conceived orders could raise concerns over the possible misuse of the Secretary’s enforcement powers. To help address those concerns, the Rule lays out a process by which entities can request clarification or reconsideration of orders issued to them.<sup>167</sup> How that process would actually function in the midst of nationwide attacks on the grid is uncertain.

However, pre-event coordination between industry and government could turn the looming threat of mandatory EO compliance into a mutually-beneficial arrangement. Rather than rely solely on adjudication mechanisms after the Secretary issues orders, DOE should collaborate with utilities to develop and refine orders in ways consistent with existing utility emergency procedures and

---

<sup>165</sup> The initial July alert was sent directly to energy sector stakeholders. See: Ellen Nakashima, “U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks,” *Washington Post*, July 8, 2017, [https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47\\_story.html?utm\\_term=.6ba8bdc7d36f](https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?utm_term=.6ba8bdc7d36f). FBI and DHS later released a public alert in October 2017. See: “Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Readiness Team*, October 20, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-293A>. For the CrashOverride alert, see: “Alert (TA17-163A) CrashOverride Malware,” *United States Computer Emergency Readiness Team*, June 12, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-163A>.

<sup>166</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1182.

<sup>167</sup> *Ibid.*, at pp. 1181-1182.

operational constraints. Doing so would – ideally – transform the mandatory nature of EOs into an advantage for utilities rather than a potential problem by leveraging the benefits that EOs provide for actions that these utilities would ordinarily carry out to protect or restore their systems. As examined in the two following sub-sections, those benefits include indemnification from environmental and other regulatory requirements, and the potential to recover costs incurred while carrying out the orders. With proper consultation, mandatory EOs could therefore serve to protect and compensate utilities for the very emergency actions required to protect their own systems.

The mandatory nature of EOs would also strengthen industry-wide security measures. NERC-developed (and FERC-approved) mandatory reliability standards and requirements to protect critical infrastructure from cyber and physical threats already help protect grid reliability against attacks by providing for consistent, nationwide adherence to those standards and the planning, training, and exercising requirements they entail. Some utilities voluntarily take further measures necessary to protect their systems from cyber threats. However, due to the interconnected nature of the BPS, the grid is only as strong as its weakest links.<sup>168</sup> The disparity in BPS entities' hardening efforts against adversarial threats means that even those that exceed NERC standard requirements remain potentially vulnerable. Creating mandatory emergency orders could help bridge the gap in protection against grid security emergencies, especially if BPS entities help shape those orders to go above and beyond the benefits of existing mandatory provisions for reliability.

Response operations provide an immediate opportunity to achieve such “value added” in designing EOs. The Electricity Subsector Coordinating Council serves as the principal liaison between the Federal government and the electric industry in responding to severe power outages. The Council includes entities of all ownership structures in the subsector, including investor-owned utilities, electric cooperatives, municipally-owned utilities, and federal utilities. This industry-wide representation enables the ESCC to serve as the “center of gravity” for coordinating response operations with DOE and other government partners. Moreover, after decades of use in hurricanes and other severe natural hazards, the Council's collaborative mechanisms offer a strong, industry-developed and time-tested basis for responding to grid security emergencies.

The ESCC is already adapting its response coordination mechanisms to support restoration against manmade threats – most notably by establishing a Cyber Mutual Assistance program.<sup>169</sup> Moreover, following Superstorm Sandy, investor-owned utilities (led by the Edison Electric Institute) also established new mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States under the National Response Event

---

<sup>168</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation's Electricity System: Second Installment of the QER*, January 2017, p. 1-33.

<sup>169</sup> Electricity Subsector Coordinating Council, *The ESCC's Cyber Mutual Assistance Program*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.2>.

(NRE) framework.<sup>170</sup> Both initiatives will be vital for responding to grid security emergencies that entail multi-region disruptions of the BPS.

The representative structure of the ESCC provides additional advantages for preparedness against GSEs. While only a limited number of industry CEOs service on the Council at any one time, those CEOs are able to reach out to other grid owners and operators across the United States and help coordinate the provision of restoration personnel and equipment on a nationwide basis. These CEOs can also request additional resources and strategic guidance when available response assets are stretched thin. However, all such assistance is voluntary; the ESCC lacks the authority to require utilities to provide assistance or to prioritize restoration operations when available resources cannot meet all requests for aid.

Emergency orders could offer DOE an additional means to support industry response operations and ensure that they account for government priorities. The Department's support could be especially valuable against cyberattacks. When hurricanes strike the Gulf Coast or the Southeast, for example, utilities on the West Coast can contribute response crews, bucket trucks, and other response assets, safe in the knowledge that the storm will not affect their own service areas. Cyberattacks will create a very different environment for providing voluntary assistance. Attacks on one utility may presage an attack on all. Utility CEOs who donate scarce cyber response personnel and assets to support another company will be at risk of suffering similar attacks, and – potentially – of suffering more severe blackouts because those personnel were already committed elsewhere.<sup>171</sup> The Cyber Mutual Assistance (CMA) Program is developing specialized protocols to deal with these challenges. However, as the ESCC notes, “participation in the CMA Program, as well as any decision to respond to requests for assistance made under the CMA Program, is voluntary.”<sup>172</sup> While the emergency order process will need to take into account the risk of re-attack in cyber incidents, EOs could nevertheless mandate compliance with industry-government decisions on restoration priorities, and reinforce the subsector's voluntary system for providing assistance in National Level Events.

Utilities may also find it helpful that their actions to meet broader national priorities, which are likely to provoke intense opposition from state and local government leaders, state Public Utility Commissioners, and customers, will be Federally-mandated. In Superstorm Sandy and other severe weather events, governors have sometimes been reluctant to support the flow of power restoration crews and equipment to neighboring states until all of their own citizens (read: voters) had their lights back on. Cyber and physical attacks on the grid could create still stronger political disincentives to share restoration assets, especially if adversaries use information warfare to inflame citizen fears over potential outages and threats to public safety. Such attacks could also put utility CEOs in the unenviable position of having to manage shortfalls in available

---

<sup>170</sup> Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, October 2016,

[http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA\\_101FINAL.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf).

<sup>171</sup> North American Electric Reliability Corporation, *Cyber Attack Task Force: Final Report*, March 2012, p. 29, [http://www.nerc.com/%20docs/cip/catf/12-CATF\\_Final\\_Report\\_BOT\\_clean\\_Mar\\_26\\_2012-Board%20Accepted%200521.pdf](http://www.nerc.com/%20docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf).

<sup>172</sup> Electricity Subsector Coordinating Council, *The ESCC's Cyber Mutual Assistance Program*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.2>.



power by depriving lower priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The Secretary of Energy can give CEOs political top cover for taking such unpopular actions, rather than leave utility leaders to act on a voluntary basis and bear the full brunt of explaining why they did so – or have them not serve national priorities at all.

## **2. Environmental, Regulatory, and Legal Waivers**

In amending the Federal Power Act to address grid security emergencies, Congress also provided power companies with an important protection for complying with emergency orders – one which they might not receive by implementing conservative operations or other emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate grid reliability standards approved by the Federal Energy Regulatory Commission (FERC) or other rules or provisions under FPA, the Act specifies that those actions “shall not be considered a violation” of those provisions. Such waivers of enforcement apply unless a complying entity acts in a “grossly negligent manner.”<sup>173</sup>

The FAST Act amendments to the FPA also introduced broader protections into section 202(c) which absolve entities from violations of Federal, state or local environment law or regulation that occur as a result of complying with an order. That provision also shields complying entities from “any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation.”<sup>174</sup> These protections also apply to Section 215A emergency orders.<sup>175</sup>

These waivers will be especially valuable for certain types of emergency orders. For example, if the Secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service could also violate FERC-approved reliability standards. Separating pre-planned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards.

The waiver process under the FPA is structured to function smoothly and automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that, in the course of complying with an emergency order, a BPS entity has acted in “a grossly negligent manner.” Nevertheless, specifying the waiver protections provided by a given EO, specific to what the Secretary is ordering entities to do, could benefit the collective response to grid security emergencies. In particular, identifying the protections provided by the EO would give complying entities assurances of their protection, and limit potential disputes with regulatory bodies.

Moreover, for certain types of emergency orders, pre-planning for regulatory waivers could comprise a necessary component of the order development process. For example, the amended

---

<sup>173</sup> 16 U.S.C. § 824o–1, Section (f)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>174</sup> 16 U.S.C. § 824a, Section (c)(3), <https://www.law.cornell.edu/uscode/text/16/824a>.

<sup>175</sup> 16 U.S.C. § 824o–1, Section (f)(2), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

FPA does not provide waivers for Nuclear Regulatory Commission (NRC) regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the NRC would enforce a violation of their regulations by a nuclear generation entity complying with an EO. The worst time to adjudicate such a dispute, however, would be in the midst of a GSE. DOE should therefore engage with the NRC to examine waiver options (or, potentially, options to exclude nuclear generators from EO requirements) as the EO development process goes forward.

Pre-planning will also be vital for EOs that accelerate power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that “the storage of strategically located spare large power transformers” and other critical grid components “will reduce the vulnerability of the United States to multiple risks facing electric grid reliability,” including cyber and physical attacks.<sup>176</sup> Accordingly, Congress required DOE to develop a Strategic Transformer Reserve Plan to determine the number and type of spare Large Power Transformers (LPTs) that should be stored, and examine issues associated with transporting those spares.<sup>177</sup>

DOE responded by providing a Strategic Transformer Reserve (March 2017) report. The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a larger pool of spare LPTs than DOE had anticipated and that a Federally-owned reserve is not needed.<sup>178</sup> However, the Plan also found that it was also crucial to ensure that LPTs can be efficiently moved during national emergencies.<sup>179</sup>

Emergency orders can play a critical role in facilitating that movement. The higher voltage classes of LPTs, including 765 kilovolt (KV) transformers, are as big as a house and can only be moved – slowly and very carefully – by specialized heavy-haul trucks, rail cars, and barges. Under the auspices of the ESCC, utilities have established a Transformer Transportation Working Group to analyze the problems posed by the emergency movement of LPTs and build collaborative plans with transportation companies and associations. A key finding of the Group’s analysis: regulatory waivers will be critical to expedite LPT movement, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.<sup>180</sup>

---

<sup>176</sup> “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1779, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>177</sup> *Ibid.*, at pp. 1780-1782.

<sup>178</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 21, <https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>179</sup> “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1781, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>180</sup> ICF (for the Department of Energy), *Assessment of Large Power Transformer Risk Mitigation Strategies*, October 2016, pp. 22-23, <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf>.

DOE's 2017 transformer report committed the Department to coordinating with the Transformer Transportation Working Group (TTWG) "to improve and optimize transportation planning in response to a significant national event impacting the electricity grid."<sup>181</sup> However, the report did not examine how emergency orders and implementation plans might speed LPT transportation. As DOE collaborates with the TTWG and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols not addressed by the FPA that pose the greatest impediments to LPT movement, and pre-plan to waive them if the President declares a GSE.

Those coordination efforts will face an immediate challenge: the Secretary of Energy lacks the statutory authority to waive key transportation regulations. Most Federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of the U.S. Department of Transportation (DOT). Federal regulations and emergency operations that would govern barge movement of transformers, which could be critical for restoring power for coastal cities and along the Mississippi-Ohio river system of inland waterways, are overseen by the U.S. Coast Guard (USCG) and the U.S. Army Corps of Engineers (USACE). State and local transportation regulations and permitting requirements will also pose major impediments to emergency LPT road movement unless adequate waivers are in place to lift them.

The EO development process should therefore include coordination with non-DOE regulatory authorities. The Department of Energy has extensive experience in collaborating with other Federal, state, local, tribal and territorial (SLTT) agencies. That experience has been especially valuable for building plans and improving coordination for restoration operations under the auspices of Emergency Response Function #12 – Energy. Moreover, as individual utilities have created contingency plans for emergency transportation with road, rail, and barge companies, they have also built relationships with SLTT agencies and government leaders. Utilities and DOE should build on those relationships and plans to launch a systematic, integrated effort to provide for regulatory waivers where (under the FPA) enforcement of violations would not automatically be waived.

Over the longer term, industry and government partners should also consider whether complying entities should have protections beyond those currently in the Federal Power Act. Prioritized load shedding for extended periods will create "winners and losers" in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other Section 9+ assets may leave dialysis centers, small urgent care centers, and facilities for special needs citizens with shortfalls in electric service. Cutting off power to lower priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.<sup>182</sup>

---

<sup>181</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 22, <https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>182</sup> Alison Frankel, "Can customers sue power companies for outages? Yes, but it's hard to win," *Reuters*, November 9, 2012, <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>.

If these risks of exposure are sufficiently severe, Congress should consider providing additional protections for BPS entities that are complying with emergency orders.

### **3. Cost Recovery for Emergency Operations and Supporting Investments in Grid Infrastructure**

Complying with emergency orders may force utilities to incur costs above and beyond their normal operating expenses. The Federal Power Act states that if FERC determines “that owners, operators, or users of critical electric infrastructure have incurred substantial costs” in complying with an EO, FERC shall “establish a mechanism that permits such owners, operators, or users to recover such costs.”<sup>183</sup> Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other EOs could require reimbursement through FERC-directed mechanisms as well.

The Act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that EOs require owners or operators of DCEI to take emergency measures, the owners or operators of critical defense facilities that rely on such infrastructure “shall bear the full incremental costs of those measures.”<sup>184</sup> Fair warning to the Department of Defense: DOD should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- Attacks create major blackouts and deprive utilities of revenue;
- Emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- Adversaries disrupt financial markets, either through direct cyberattacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.<sup>185</sup>

Power companies are rapidly strengthening their plans and capabilities for cross-sector support with the financial services sector (and with the communications sector on which they depend).<sup>186</sup> These efforts should include the development of contingency plans for financial services

---

<sup>183</sup> The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs “prudently,” and that those costs “cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users. 16 U.S.C. § 824o–1, Section (b)(6)(A), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

<sup>184</sup> 16 U.S.C. § 824o–1, Section (b)(6)(B), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

<sup>185</sup> North American Electric Reliability Corporation, *Grid Security Exercise: GridEx III Report*, March 2016, p. 15, <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.

<sup>186</sup> See, for example, the Strategic Infrastructure Coordinating Council (SICC). Electricity Subsector Coordinating Council, *ESCC Initiatives*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf>.

companies (in coordination with the Department of Treasury and DOE) to help utilities meet the time-urgent expenses of responding to grid security emergencies.

In addition, to facilitate the EO reimbursement process provided for in the Federal Power Act, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with EOs will be more difficult once attacks are underway. That is especially true since the text of the FPA leaves substantial ambiguities to resolve – starting with the definition of who are “users” of critical electric infrastructure and therefore potentially eligible for reimbursement.

Such users might well include electricity distribution companies who are not BPS entities (and are therefore not subject to emergency orders), but who could be vital to protect and restore the flow of power between high voltage transmission systems and regional hospitals and other critical facilities. For example, intentional load shedding operations to stabilize the grid are nearly all performed at the distribution level, and distribution providers would also be performing the switching for required to implement rotating blackouts. For the many BPS entities that are not vertically integrated and do not own and operate “local” distribution utilities excluded from the FPA’s BPS definition, it will be essential to include those local distribution providers in contingency plans to execute emergency orders. Given the costs that distribution systems may incur in implementing EOs, FERC and its partners should clarify eligibility for reimbursement and the process by which grid operators will recover their costs as soon as possible.

Cost recovery for investments in grid infrastructure to facilitate emergency orders will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. However, other EOs may be impossible to execute unless BPS entities make additional investments in infrastructure. For vital but remote military bases that are served by a single transmission line, it will be near-useless to order transmission operators to protect or rapidly restore service to those bases if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure they can help defeat U.S. adversaries when the Nation is under attack. DOD will need to ensure it has a cost recovery mechanism to reimburse DCEI owners for making such investments.

For pre-planned power islands to be even remotely viable as an EO design option, many such islands will also require at least some infrastructure construction. Ideally, these pre-planned islands will make use of existing generation, transmission, and distribution assets within their service footprints so that they can separate from the grid and still be able to provide reliable electric service to the Section 9+ assets insider their borders. But many areas that might be designed to function as islands in a GSE will lack adequate infrastructure to do so. The interconnected design of the grid enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Pre-planned power islands will not only lose those reliability benefits, but also have to make do with infrastructure that



utilities built and aligned to be supporting components of the interconnected grid – *not* self-sustaining islands that would be stood up in grid security emergencies. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: many EOs could require spending on new transmission lines and other grid infrastructure in order to be effectively implemented.

The provisions of the FPA pertaining to emergency orders do not explicitly authorize reimbursement for such infrastructure investments. While the Act requires FERC to establish a mechanism to enable owners, users, and operators of CEI and DCEI to recover their costs of complying with emergency orders, those funding provisions do not mention pre-attack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover their costs for infrastructure investments against cyber and physical attacks.<sup>187</sup> FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate EO execution.

Similar discussions will be valuable with state public utility commissions (PUCs). As noted above, distribution systems will likely need to play a vital role in implementing emergency orders. PUCs have primary regulatory authority over distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. Public utility commissions could also make important contributions to reviewing proposed EO implementation plans that would be executed within their respective states, particularly for orders that distribution systems would need to help implement.

The Federal Power Act opens the door to discussions with PUCs over investments and planning to support EO execution. The Act states that FERC and the Secretary of Energy “shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions.”<sup>188</sup> Initiating such discussions with the National Association of Regulated Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has conducted detailed analysis of criteria for assessing the prudence of investments against cyber and physical attacks, and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

---

<sup>187</sup> See, for example: Federal Energy Regulatory Commission (FERC), *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies*, Statement of Policy (96 FERC ¶ 61,299), September 14, 2011; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), April 19, 2004, pp. 10-11 (2004); FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), September 22, 2016, p. 60.

<sup>188</sup> 16 U.S.C. § 824o–1, Section (d)(4), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

## **V. CONCLUSIONS AND RECOMMENDATIONS FOR FOLLOW-ON ANALYSIS**

[To be completed by April 30, 2018]

**From:** [Peter Pry](#)  
**To:** [Joseph McClelland](#)  
**Subject:** NEW BOOK--EMP MANHATTAN PROJECT  
**Date:** Wednesday, August 22, 2018 4:51:38 PM  
**Attachments:** [MANHATTANbook.PDF](#)

---

Joe—Attached find my new book with an Introduction by Dr. William Graham, former White House Science Advisor to President Reagan and Chairman of the Congressional EMP Commission, “EMP MANHATTAN PROJECT: Organizing Survival Against An Electromagnetic Pulse Catastrophe” (minus the front and rear covers). Soon available in hard-copy from Amazon.com —Peter



From: [Joseph McClelland](#)  
To: [\(b\) \(6\)](#); [Andrew Dodge](#)  
Cc: [David Andrejcek](#); [Harry Tom](#)  
Subject: Draft Study on Grid Security Emergencies  
Date: Friday, April 27, 2018 6:47:41 AM  
Attachments: [APL GSE Study Sections I-IV April 26 2018.docx](#)  
[ATT00001.htm](#)

---

Are you folks in today and available to discuss this study? I'd like for you to read over it and provide any suggestions (not detailed edits) to its content.

Thanks,

Joe



*DRAFT: NOT FOR USE OR CITATION  
WITHOUT PERMISSION OF THE AUTHOR*

# **RESILIENCE FOR GRID SECURITY EMERGENCIES: OPPORTUNITIES FOR INDUSTRY-GOVERNMENT COLLABORATION**

Paul N. Stockton (pstockton@sonecon.com)  
Report for the Johns Hopkins University Applied Physics Laboratory (APL)  
April 26, 2018

## **EXECUTIVE SUMMARY**

The United States Congress has opened the door to novel strategies for defending the U.S. electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act in December 2015, Congress granted the Secretary of Energy vast new authorities to use when the President declares that a grid security emergency exists. Most important, legislators authorized the Secretary of Energy to issue emergency orders to grid owners and operators to protect and restore grid reliability when attacks on their systems are imminent or underway.<sup>1</sup> The Federal Power Act is silent, however, on what the Secretary might order these owners and operators to do and how emergency orders can effectively bolster their protection efforts.

The onslaught of an attack would be the worst possible time to develop such orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid which could then be adjusted to fit the specific circumstances of an attack. Developing such orders in advance would help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. In turn, those contingency plans could provide the basis for training and exercise initiatives to prepare for the attacks to come.

This study is structured help the electricity subsector partner with the Department of Energy (DOE) to develop emergency orders and meet the broader policy and operational challenges that grid security emergencies will entail. In particular, the study examines how these partners might develop emergency orders to protect grid reliability against potentially catastrophic cyber and physical attacks, and – if major blackouts occur – help utilities accelerate the restoration of power.

---

<sup>1</sup> The "Fixing America's Surface Transportation Act" [hereinafter referred to as the FAST Act], Public Law 114-94, *U.S. Statutes at Large* 129 (2015): pp. 1773-4, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

DOE and their industry partners should develop emergency orders for three possible phases of grid security emergencies. The Federal Power Act specifies that the President can declare a grid security emergency (GSE) when there is “imminent danger” of an attack on electric infrastructure critical for national defense, economic security, and public health and safety. Strong foundations already exist for developing emergency orders for this initial, pre-attack phase of GSEs. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions, such as staffing up emergency operations centers, increasing available generation to help manage grid instabilities, and taking other precautionary measures.

Determining that a cyber or physical attack is imminent could be vastly more difficult than doing so for hurricanes. However, if the United States has sufficient warning of an attack, many of the same measures used to bolster preparedness against natural hazards might be adapted to provide pre-attack options for conservative operations. Promising opportunities also exist to develop measures tailored for cyber or physical threats. Emergency orders for conservative operations constitute “low hanging fruit;” industry and government partners should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The Federal Power Act also states that the President can declare a GSE when attacks are “occurring.” Industry and government partners should develop a second set of orders to use once attacks are underway, both to prevent power failures from cascading across the United States and to sustain electric service to major regional hospitals and other critical facilities. Existing electric industry plans and capabilities provide a strong basis to develop such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Emergency orders for equivalent *extraordinary measures* could provide useful “arrows in the quiver” in grid security emergencies, and could help integrate national security priorities into existing utility plans to counter grid instabilities.

A third set of potential emergency orders would help utilities accelerate power restoration if blackouts occur. Attacks that damage or destroy large number of high voltage transformers or other difficult-to-replace equipment could create outages that darken major portions of the United States for many weeks or even months. Power companies and DOE already have initiatives underway to meet this challenge. They should also collaborate to develop emergency orders to *accelerate restoration*. In particular, orders might be drafted to account for the risk that adversaries will continue attacking after their initial salvo, and launch follow-on strikes to disrupt restoration operations and lengthen U.S. power outages.

Of course, Russia, China, and other potential adversaries will not strike the grid merely to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to U.S. Defense installations, ports, and other civilian infrastructure essential for deploying and sustaining forces to the region. Emergency orders can be designed to help deter – and, if necessary, defeat – such attacks. This study proposes specific

options to do so, in support of the *National Security Strategy of the United States of America* and other sources of U.S. policy guidance.

The study also identifies ways that government and industry can pre-plan to communicate with the American people if adversaries strike. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks – and, potentially, attack the phone and internet-based communications systems on which utilities typically use coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications “playbooks” to prepare for grid security emergencies, and make doing so a core component of the emergency order development process.

These partners should also pre-plan to take advantage of an especially valuable way in which Congress amended the Federal Power Act: the creation of new provisions for emergency regulatory waivers and cost recovery for power companies. Legislators recognized that to comply with emergency orders, grid owners and operators might have to violate environmental regulations and other standards. The Act now protects entities from the enforcement of such violations if they occur as the result of complying with emergency orders. The FPA also provides for the recovery of costs that companies will incur in implementing those orders. This study suggests additional measures that industry and government may want to consider to facilitate compliance and reinforce the “value added” of emergency orders for countering attacks on the grid.

In addition, government and industry partners should examine the triggers and thresholds for declaring grid security emergencies and issuing emergency orders. Major ambiguities surround the criteria for making such declarations, especially for attacks that may be imminent. One option to clarify these criteria would be to leverage the electric industry’s focus on preserving “adequate levels of reliability,” and declare emergencies when adversaries are poised to create cascading power failures and other major disruptions across multiple states. However, the President should also retain the flexibility to declare GSEs for a broad range of other contingencies.

Industry and government partners should also identify opportunities to build broader resilience for grid security emergencies. Intensive follow-on work will be required to finalize the development of emergency orders and build utility-specific contingency plans to implement them in ways that account for accelerating structural changes in the electricity subsector (including the large-scale integration of wind and solar generation). Those collaborative efforts will require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, three additional opportunities for progress could offer special benefits for strengthening GSE preparedness. First, DOE and its industry partners should consider expanding the scope of EO planning across the energy sector to address the risk that adversaries will attack

both the grid and the natural gas transmission system on which power generation increasingly depends. Second, these partners should develop additional options to counter the risk that adversaries will conduct targeted information operations to sow disorder and magnify the disruptive effects of attacks on the grid. Third, government leaders should also explore strategic opportunities to capitalize on the improvements in grid resilience that EOs and related preparedness initiatives will make possible. In particular, these leaders should consider developing integrated offense-defense operational plans to strengthen the deterrence of cyberattacks against the United States, and to help manage the escalation (and speed the favorable resolution) of conflicts that do occur.

## **I. DEVELOPING EMERGENCY ORDERS UNDER THE FEDERAL POWER ACT: OVERARCHING GOALS AND DESIGN REQUIREMENTS**

The foundational importance of the electric grid makes it a prime target for attack. As Secretary of Energy Richard Perry emphasizes, “America’s greatness depends on a reliable, resilient electric grid” that can power the economy, support national defense, and provide for the necessities of modern life.<sup>2</sup> To prevent adversaries from exploiting this extraordinary dependence on the U.S. electric system, the Department of Energy and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter – and, if necessary, defeat – attacks on the grid.<sup>3</sup>

The text of the FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the “FAST Act” amendments to the FPA, legislators greatly expanded the Secretary of Energy’s authority to issue emergency orders to grid owners and operators. Under Section 215A of the Act, “the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgement of the Secretary to protect or restore the reliability” of the critical grid infrastructure in a grid security emergency.<sup>4</sup>

---

<sup>2</sup> Secretary of Energy Richard Perry, *Letter to the Federal Energy Regulatory Commission Re: Secretary of Energy’s Direction that the Federal Energy Regulatory Commission Issue Grid Resiliency Rules Pursuant to the Secretary’s Authority Under Section 403 of the Department of Energy Organization Act*, September 28, 2017, <https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf>.

<sup>3</sup> As noted above, the 2015 FAST Act amendments to the Federal Power Act (FPA) provide the authority to do so. Prior to 2015, Section 202(c) of the FPA already authorized the Secretary of Energy to issue emergency orders to order “temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest.” That provision also specified that the Secretary could exercise such powers “during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes.” See: “DOE’s Use of Federal Power Act Emergency Authority,” *Department of Energy*, 2017, <https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use>. The 2015 FAST Act amendments to the FPA gave the Secretary further powers (mostly incorporated in Section 215A of the Act), which are the primary focus of this study.

<sup>4</sup> Before the Secretary can issue emergency orders, the President must first declare a grid security emergency (GSE). The analysis that follows examines the definition of GSEs in the FPA. This analysis also examines the focus of

However, legislators provided only limited guidance on what the Secretary might order power companies to do. The Department of Energy and their partners in the electricity subsector have begun to assess which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats.

This portion of the study (Section I) examines the near and longer-term advantages of developing emergency orders before adversaries strike. Section I also identifies specific industry and government partners who might participate in this development process, and highlights the overall design requirements that emergency orders may need to meet, both to comply with the Federal Power Act and to address the broader challenges that grid security emergencies will pose.

The Act specifies that before the Secretary can issue emergency orders, the President must first declare a grid security emergency (GSE). Section II surveys the types of threats that can trigger a GSE and explains why this study focuses on the risk of cyber and physical attacks. Section II also examines possible thresholds and decision criteria that the President might use to determine whether a GSE exists, and how consultations and information sharing with power companies might support such determinations.

Section III provides a framework for developing emergency orders for use in three phases of GSEs: when the President determines that there is an imminent danger of attacks, when attacks are underway, and when electric companies are restoring power – potentially in the face of continuing attacks on the grid. Section III also provides examples of emergency orders (EOs) and identifies promising options for further analysis.

Section IV analyzes the broader design challenges that emergency orders may entail. These include: 1) tailoring EOs to help deter attacks on the United States, and help the U.S. military defeat adversaries if deterrence fails; 2) ensuring that the Secretary can effectively communicate emergency orders to power companies if phone and internet communications are disrupted, and pre-planning to communicate with the American people when attacks are underway; and 3) strengthening the “value added” of emergency orders for the electric industry by providing political top cover for unpopular emergency measures, as well as regulatory waivers and cost recovery beyond the provisions in the FPA. Section V identifies issues for further analysis that may offer special benefits for building preparedness for grid security emergencies.

## **A. IMPERATIVES FOR GOVERNMENT-INDUSTRY COLLABORATION**

The Secretary’s new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, “the nine most terrifying words in the English language are

---

emergency orders on protecting or restoring the reliability of critical electric infrastructure and defense critical electric infrastructure in the bulk power system (BPS), and the definition of these terms in the Act.



‘I’m from the government and I’m here to help.’”<sup>5</sup> Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already beginning to manage such risks by incorporating industry recommendations on the process by which the Secretary should issue emergency orders (EOs), and – “if practicable” – consult with industry before those orders are issued.<sup>6</sup> The next collaborative step should be to include power companies in designing EOs. Grid owners and operators have unequalled knowledge of their own infrastructure and operating procedures, and have extensive experience in employing emergency measures to protect and restore grid resilience. They are well-positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses – and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders will assist them in protecting or restoring grid reliability, above and beyond the emergency measures that companies would already be taking on their own.

Industry will need government leadership as well. Federal guidance will be essential to ensure that emergency orders help achieve overarching U.S. security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing EOs to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.<sup>7</sup> Federal leadership will also be necessary to integrate criteria and decisions for issuing emergency orders into the broader U.S. incident response system established by Presidential Policy Directive 41: *United States Cyber Incident Coordination* (July 2016), the *National Response Framework* (June 2016), and other mechanisms and guidelines for coordinating response operations.<sup>8</sup> In addition, as provided for in the FPA and other sources of Federal guidance, government agencies (with industry support) will also need to identify the grid infrastructure that is most critical for protecting the U.S. economy, public health and safety, and the defense of the United States.<sup>9</sup>

Government participation will also be necessary to account for the support that DOE and other agencies may be able provide to industry in grid security emergencies. For example, if adversaries destroy large power transformers and other critical grid infrastructure, Federal, state,

---

<sup>5</sup> Ronald Reagan, “The President’s News Conference,” August 12, 1986, <http://www.presidency.ucsb.edu/ws/?pid=37733>.

<sup>6</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1176; EEI, “COMMENTS OF THE EDISON ELECTRIC INSTITUTE,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*, February 6, 2017; and IRC, “ISO-RTO Council Comments on Notice of Proposed Rulemaking,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*, February 6, 2017.

<sup>7</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017.

<sup>8</sup> White House, *Presidential Policy Directive - United States Cyber Incident Coordination*, July 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>; Department of Homeland Security, *National Response Framework: Third Edition*, June 2016.

<sup>9</sup> 16 U.S.C. § 824o-1, Section (c), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

local, tribal, and territorial transportation agencies may be able to waive regulations and other requirements that would otherwise slow the movement of replacement transformers. The Department of Energy may not be able to order transportation agencies to issue such waivers. However, DOE can lead government-wide engagement to incorporate waiver planning and other support functions into emergency orders and provide a focal point for industry collaboration.<sup>10</sup> Most important of all: DOE is the Sector-Specific Agency for the energy sector and is uniquely positioned to partner with electric utilities in the EO development process.

## **1. Drafting Template Emergency Orders Before Attacks Occur**

The Federal Power Act specifies that before issuing emergency orders “the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action,” consult with appropriate power companies and other stakeholders in grid resilience.<sup>11</sup> In January 2018, the Department of Energy issued procedures for conducting such consultations and communicating emergency orders, and incorporated a number of recommendations proposed by power companies to strengthen industry-government coordination in grid security emergencies.<sup>12</sup>

But the need for action may be too urgent to permit such consultation before the Secretary issues emergency orders. Adversaries may launch cyberattacks on the grid with little or no warning. Indeed, they will have additional incentives to do so if they can preclude the effective use of emergency orders by minimizing opportunities for industry-government dialogue, and by disrupting communications between DOE and grid owners and operators.

To ensure that EOs will benefit from industry-government consultation, and to minimize the risk that DOE will have to design orders from scratch amidst the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, Assistant Secretary of Energy for Electricity Delivery and Energy Reliability, stated in March 2018 that “In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.”<sup>13</sup> Power companies and other

---

<sup>10</sup> The FAST Act amendments explicitly provide for such a role in cybersecurity planning and incident management. See: “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1779, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>11</sup> 16 U.S. Code § 824o-1, <https://www.law.cornell.edu/uscode/text/16/824o-1>. See also the notice of proposed rulemaking and request for comment: Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 81, No. 235 (2016), [https://energy.gov/sites/prod/files/2017/02/f34/DOE\\_FRDOC\\_0001-3281.pdf](https://energy.gov/sites/prod/files/2017/02/f34/DOE_FRDOC_0001-3281.pdf).

<sup>12</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1175.

<sup>13</sup> Bruce J. Walker, *Written Testimony Before the U.S. Senate Committee on Energy and Natural Resources*, March 1, 2018, [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=1C574731-A9C0-4E1C-9E05-15C492E332B1](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1)

electricity subsector organizations have also emphasized the need for industry and government to jointly develop orders before adversaries strike.<sup>14</sup>

Such collaborative efforts should initially focus on creating *template orders*: i.e., orders that lay out the basic types of actions that the Secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act’s potential value for the Secretary to issue general orders to “protect and restore the reliability of the grid.” Vague, overly broad directives cannot provide an adequate basis for utilities to build system-specific plans to implement them, or exercise and train utility personnel to do so. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for “maximum generation” and increased reserve margins to more aggressive, far-reaching measures.<sup>15</sup> The goals for such development efforts: 1) provide a menu of pre-agreed upon options from which the Secretary can choose as circumstances require, in consultation with industry (as provided for in the FPA); and 2) ensure that existing utility plans for prioritized power restoration and other emergency operations help achieve government-identified national security priorities.

In actual attacks, Russia, China, or other potential adversaries will employ country-specific malware and tactics, techniques, and procedures. Defense against those attacks will require equally tailored, threat-specific tactical and operational response measures. Over time, it may be possible to develop (and protect adversaries from stealing) emergency orders that account for these individualized defensive requirements. U.S. leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this study will examine the development of such integrated offense-defense plans as a future research priority.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military

---

<sup>14</sup> See: Joint Commenters, “COMMENTS OF AMERICAN PUBLIC POWER ASSOCIATION, LARGE PUBLIC POWER COUNCIL, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, AND TRANSMISSION ACCESS POLICY STUDY GROUP,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, February 23, 2017, <http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf>; NASEO, “COMMENTS OF THE NATIONAL ASSOCIATION OF STATE ENERGY OFFICIALS,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, n.d.a, [https://www.naseo.org/Data/Sites/1/naseo-comments\\_rin-1901-ab40.pdf](https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901-ab40.pdf); and EEI, “COMMENTS OF THE EDISON ELECTRIC INSTITUTE,” *In Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40)*, February 6, 2017.

<sup>15</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help “maintain reliable operation while meeting ... unexpected outages of existing capacity.” See: NERC, “M-1 Reserve Margin,” 2017, <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.

bases, regional hospitals, and other critical facilities in their service area that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and present opportunities to improve order design and coordination. Training programs to prepare employees to carry out utility-specific plans to implement template orders should also get underway as soon as those orders are developed. On a larger scale, utilities will also be able to plan and exercise for the employment of template emergency orders under the Cyber Mutual Assistance (CMA) program. This program enables over a hundred utilities to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.<sup>16</sup> As the CMA program grows, it will provide increasingly valuable support for the nationwide execution of emergency orders.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the Secretary of Energy has the sole authority to issue EOs, the Secretary may request input from senior DOE staff on the benefits of specific options and the rationale for issuing those orders. The Secretary and DOE staffers may also need to brief the President and the National Security Council on proposed orders and the public messaging issues the orders entail. By developing EOs before GSEs occur and explaining how they will protect grid reliability, DOE and industry partners can strengthen the foundations for such deliberations and help design exercises for GSE decision making.

Over the longer term, industry and government leaders might structure their collaboration in order to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public-private and interagency coordination.<sup>17</sup> Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government-industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, the development of template emergency orders and contingency plans to implement them will require power companies to conduct extensive operational and engineering studies. The FAST Act amendments to the FPA provide no funding for such development efforts.

---

<sup>16</sup> “The ESCC’s Cyber Mutual Assistance Program,” *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1>.

<sup>17</sup> Richard Danzig, “Catastrophic Bioterrorism – What Is To Be Done?,” *Center for Technology and National Security Policy*, August 2003, [http://www.response-analytics.org/images/Danzig\\_Bioterror\\_Paper.pdf](http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf), pp. 5-7; Blue Ribbon Study Panel on Biodefense (Hudson Institute), *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts – Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*, October 2015, <http://www.biodefensestudy.org/a-national-blueprint-for-biodefense>, pp. 13 and 42-4.

Moreover, in order to build and effectively execute such plans, power companies will need to coordinate (and potentially share sensitive information) with a much wider array of partners as the development process goes forward.

## **2. The Bulk Power System as the Focus of GSE Declarations and Emergency Orders: Implications for EO Development**

Before examining these design requirements in further detail, an underlying constraint in the Federal Power Act merits analysis. The Act specifies that critical electric infrastructure includes only those assets that comprise the bulk power system (BPS). BPS assets are those “facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation facilities needed to maintain transmission system reliability.”<sup>18</sup> These bulk power system generation and transmission assets provide synchronized power across the three interconnections that serve the entire United States and parts of Mexico and Canada.<sup>19</sup>

However, as defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.<sup>20</sup> The FPA also specifies that emergency orders will apply to BPS owners and operators. That focus excludes local distribution providers, even if they provide the “last mile” of connectivity between transmission systems and military bases and other critical customers. The exclusion of local distribution providers has significant implications for the design and implementation of EOs, and poses political as well as technical challenges for protecting and restoring electric service.

The FPA states that the Secretary of Energy may issue emergency orders to a range of BPS “entities.”<sup>21</sup> These include:

***a. The Electric Reliability Organization.*** After blackouts cascaded across major portions of the United States in August 2003, Congress directed the Federal Energy Reliability Commission (FERC) to designate an Electric Reliability Organization (ERO) to enforce mandatory electric reliability rules on all users, owners, and operators of the U.S. bulk power system.<sup>22</sup> FERC appointed the North American Electric Reliability Corporation (NERC) as the first ever ERO in July 2006, and it has served in that role since.<sup>23</sup> NERC’s mission is to assure the reliability and

---

<sup>18</sup> 16 U.S.C. § 824o, Section (a)(1), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>19</sup> Interconnections are defined as the “geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control.” North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See: “Glossary of Terms Used in NERC Reliability Standards,” *NERC*, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

<sup>20</sup> The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify “local” distribution. See: 16 U.S.C. § 824o, Section (a), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>21</sup> 16 U.S.C. § 824o–1, Section (b)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>22</sup> *Energy Policy Act*, Public Law 109-58, *U.S. Statutes at Large* 119 (2005): pp. 942-943.

<sup>23</sup> NERC, *History of NERC*, August 2013, <http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf>.

For more information on NERC, see: “About NERC,” *NERC*, n.d.a, <http://www.nerc.com/AboutNERC/Pages/default.aspx>.



security of the BPS in North America. As such, NERC will be a key partner in developing template emergency orders, especially to help defeat attacks that could create cascading blackouts or other multi-state disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a critical role for the electric subsector in establishing situational awareness, incident management and coordination, and communication capabilities.<sup>24</sup> E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be particularly vital in consultations on issuing and refining emergency orders against specific threats.

***b. Regional entities responsible for enforcing reliability standards for the bulk power system.***<sup>25</sup> NERC delegates its authority to monitor and enforce compliance with reliability standards to eight regional entities which “account for virtually all the electricity supplied in the United States.”<sup>26</sup> While regional entities play crucial oversight roles, they do not directly operate the grid and would not, on their own, be positioned to execute emergency orders to protect or restore reliability. They will nonetheless play an important role regarding waivers for legal and regulatory compliance, as will be examined in detail in Section IV.

***c. Owners, users and operators of critical electric infrastructure (CEI) or defense critical electric infrastructure (DCEI) within the United States.***<sup>27</sup> When the President declares a grid security emergency, issuing emergency orders to power companies that own and operate generation and transmission assets will offer crucial opportunities to protect grid reliability. In addition, Reliability Coordinators (RCs) will play essential roles in designing and implementing emergency orders. RCs are the entities that constitute “the highest level of authority” for the reliable operation of the bulk electric system.<sup>28</sup> RCs are also responsible for maintaining a “wide

---

<sup>24</sup> “Electricity ISAC,” NERC, n.d.a, <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>25</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177. See also: 16 U.S.C. § 824o, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>26</sup> “Key Players,” *North American Electric Reliability Corporation*, n.d.a., <https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>. One regional entity, however, announced its intention to dissolve in July 2017, currently pending final FERC approval. See: North American Electric Reliability Corporation, “JOINT PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION, MIDWEST RELIABILITY ORGANIZATION, AND SERC RELIABILITY CORPORATION FOR APPROVALS IN CONNECTION WITH THE DISSOLUTION OF THE SOUTHWEST POWER POOL REGIONAL ENTITY,” *Filing Before the Federal Energy Regulatory Commission* (Docket No. RR18-3-000), <https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/SPP%20Dissolution%20Petition.pdf>.

<sup>27</sup> The analysis that follows later in this section examines the definition of “users” of critical electric infrastructure, as well as defense critical electric infrastructure.

<sup>28</sup> While the Bulk Power System (BPS) broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the Bulk Electric System (BES) is a subset of the BPS which includes, with some exclusions, all transmission and real and reactive power sources at 100 kV or higher. As with the BPS, the BES definition excludes local distribution providers. For these definitions, as well as the definition of Reliability Coordinators, see: “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf). Consistent with the FPA and the authorities it provides for

area view” of the bulk electric system, and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, RCs will be critical for designing, receiving, and implementing emergency orders to counter attacks that may exceed the ability of individual BPS system owners and operators to defeat. Seven Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) also help operate and ensure the reliability of the bulk electric system in many regions of the United States.<sup>29</sup> Accordingly, RTOs and ISOs will be essential to the design and execution of emergency orders.

#### ***d. Local Distribution Providers***

The role of distribution systems in responding to grid security emergencies is less clear-cut. As noted above, the Federal Power Act only authorizes the Secretary to issue emergency orders to bulk power system entities. The Act does not explicitly authorize the Secretary to issue emergency orders to utilities that provide for local distribution of electric power. Nevertheless, local distribution infrastructure may play a vital role in protecting the flow of power to key facilities in grid security emergencies. Even if emergency orders can help defeat attacks on the bulk power system, adversaries may still be able to achieve catastrophic effects by attacking multiple local distribution systems, and thereby interrupt the flow of power from transmission systems to hospitals and other end users. A holistic approach to GSE preparedness will need to account for these risks to local infrastructure.

Integrating local distribution systems into planning for grid security emergencies will also be useful from an operational perspective. Even though local distribution utilities may not themselves be subject to EOs, they may be functionally required to help implement such orders. For example, if the Secretary orders transmission systems to shed load to protect grid reliability, while also preserving the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding.

From an historical perspective, it is understandable why the FPA does not explicitly account for local distribution utilities in grid security emergency operations. State public utility commissions have long had regulatory jurisdiction over distribution systems. Any legislative effort to give the Secretary of Energy emergency authorities over local distribution assets could have created strong opposition from state leaders and their defenders in Congress.<sup>30</sup> Nevertheless, if the

---

handling grid security emergencies, this study focuses on the application of emergency orders to BPS entities specifically.

<sup>29</sup> There are 10 RTOs and ISOs under NERC’s purview, though three operate exclusively in Canada. RTOs and ISOs are independent, membership-based, non-profit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are operated by individual utilities or utility holding companies. “About 60% of the U.S. electric power supply is managed by RTOs,” *U.S. Energy Information Administration*, April 4, 2011, <https://www.eia.gov/todayinenergy/detail.php?id=790>. Six of the seven RTOs/ISOs are also current reliability coordinators. See: “Reliability Coordinators,” *North American Electric Reliability Corporation*, n.d.a., <https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.

<sup>30</sup> The U.S. Constitution, in most cases, only allows Federal regulation of private economic activity for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See: Jim Lazar (for The Regulatory Assistance Project), *Electricity Regulation in the US: A Guide*, 2<sup>nd</sup> Edition, June 2016, p. 15.

United States is to prevent grid-wide attacks from jeopardizing national security, economic security, or public health or safety, extensive coordination and collaboration with local distribution systems will be essential.

An initial step toward building such an integrated approach will be to specify which distribution facilities that serve CEI and DCEI are “local.” As FERC notes, the FPA’s BPS definition “does not establish a voltage threshold limit of applicability or configuration.” The definition instead relies on the functional requirement of “necessary for operating an interconnected electric energy transmission network” set out by the FPA.<sup>31</sup>

Local distribution utilities which are not necessary for such interconnected operations may nevertheless provide the “last mile” of power delivery to military bases and other vital facilities. It might be possible to interpret the FPA as making emergency order applicable to these utilities as well. The Act states that emergency orders may apply to “any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure” within the United States. The Act, however, does not further define owners, users and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the Act.

Even if the Secretary cannot issue orders directly to such utilities, BPS entities should still include them in building the contingency plans necessary to implement emergency orders. Before BPS owners and operators receive EOs, they could pre-plan to coordinate with local distribution systems to strengthen comprehensive, end-to-end protection of grid reliability for critical customers. Many companies that own transmission assets also own distribution infrastructure, simplifying coordination for EO planning purposes. Integrated planning will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for “vertically integrated” utilities that own and operate assets for all three functions.

However, while many investor-owned utilities are vertically integrated, municipally-owned electric utilities and rural electric cooperatives (which serve a significant amount of CEI and DCEI) are not. In the many regions of the United States where generation, transmission, and distribution systems exist as separate, non-integrated companies, additional engagement

---

<sup>31</sup> Federal Energy Regulatory Commission, *Revision to Electric Reliability Organization Definition of Bulk Electric System* (Order No. 743), 133 FERC ¶ 61,150, November 18, 2010, pp. 22-24. FERC and NERC have also defined the Bulk Electric System (BES), a subset of the BPS, for regulatory purposes. Unlike the FPA’s BPS definition, NERC’s core BES definition establishes a uniform “bright line” threshold of 100 kV. Accordingly, the BES includes “all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher,” with specific, additional criteria for inclusions and exclusions to provide further clarity. NERC also established an exception process through their Rules of Procedure to make additional inclusions and exclusions on a case-by-case basis. FERC accepted the definition in 2012 (Docket Nos. RM12-6-000 and RM12-7-000; Order No. 773), and the FERC decision was upheld by the Second Circuit Court of Appeals, in *New York V. FERC*, 783 F.3d 946 (2d Cir. 2015). See: Federal Energy Regulatory Commission, *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure* (Order No. 773-A), 143 FERC ¶ 61,053, April 18, 2013, pp. 2-7; and “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

measures will be essential to help effectively implement EOs. As the Federal government identifies critical facilities for prioritized protection and restoration of power, BPS entities that provide the electricity on which those facilities rely should ensure that local distribution systems are included in designing and implementing orders for prioritized emergency service.

#### *e. Additional Partners for Engagement*

As the Department of Energy and the electricity subsector develop emergency orders, they should identify and pre-plan with other partners who can assist in executing those orders. The GSE Rule notes that “Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits” to expedite the restoration of power.<sup>32</sup> Still broader collaboration with government and private sector partners may be valuable for implementing EOs to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy Large Power Transformers (LPTs) at substations across the United States, and these attacks cut off power to critical military bases, the Secretary might order industry to prioritize the replacement of LPTs at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program (STEP) to provide for such replacements,<sup>33</sup> and new industry-led organizations such as Grid Assurance and the Regional Equipment Sharing for Transmission Outage Restoration Agreement (RESTORE – a mutual assistance-like agreement for enabling transfers of transformers and other critical equipment recently approved by FERC).<sup>34</sup> These initiatives further strengthen the industry’s LPT resilience posture in ways that could be valuable for restoration operations in grid security emergencies.

However, power companies do not move LPTs by themselves. They rely on railroad companies, barges, and “heavy hauler” trucking companies to help do so, and have established a Transformer Transportation Working Group (TTWG) to plan and coordinate LPT movement operations.<sup>35</sup> The FPA does not give the Secretary authority to issue orders to transportation companies. Nevertheless, in anticipation of orders for transformer movement, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Pre-coordinating with the U.S. Department of Transportation and state governments to get permits and regulatory waivers to expedite transformer movement will also be helpful.

---

<sup>32</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177.

<sup>33</sup> See: Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>; and “Spare Transformers,” *Edison Electric Institute*, n.d.a, <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.

<sup>34</sup> Federal Energy Regulatory Commission, *ORDER AUTHORIZING ACQUISITION AND DISPOSITION OF JURISDICTIONAL FACILITIES* (163 FERC ¶ 61,005), April 3, 2018, p. 10, <https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf>.

<sup>35</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 12, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

Equally valuable partnership opportunities will emerge in designing and pre-planning for the execution of other emergency orders. For example, when the Secretary issues an emergency order, agencies and utilities should already have determined what they will tell the public about the purpose of the order, its expected impact on electric service, and -- ideally -- when normal service will be restored. Identifying these and other partnership requirements will be critical as the design process goes forward.

### **3. Template Emergency Orders: Goals and Specific Design Requirements**

The starting point to develop template emergency orders is to identify the objectives and design requirements that these orders will need to encompass, and clarify the underlying policy challenges that the EO development process will need to address. Key issues analyzed in the next sections of the study:

- Threats, Triggers and Thresholds for Issuing Emergency Orders. The Federal Power Act requires the President to have declared a “grid security emergency” (GSE) before the Secretary can issue emergency orders.<sup>36</sup> Only a limited number of natural and manmade hazards can trigger a GSE. Countering each of those hazards will require different, threat-specific specific emergency orders. Hence, the first step for developing such orders will be to select the threats on which the design process should focus.

The Act authorizes the President to declare a GSE when there is an “imminent danger” of attacks on critical grid infrastructure, or when attacks are occurring.<sup>37</sup> Different types of emergency orders will be needed to preserve grid reliability 1) when attacks are imminent, and 2) when attacks are underway. Promising opportunities also exist to develop orders for a third phase of GSE operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.

- Incorporating National Security Policies and Priorities into GSE Order Design. The FPA’s definition of grid security emergencies helps frame the order design process in an additional way. GSEs exist when adversaries pose serious threats to:
  - *Critical electric infrastructure*, which is comprised of grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters;”<sup>38</sup> and
  - *Defense critical electric infrastructure*, which serves facilities that are “critical to the defense of the United States” and are vulnerable to the disruption of grid-provided power.<sup>39</sup>

---

<sup>36</sup> Along with cyberattacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>37</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>38</sup> 16 U.S.C. § 824o–1, Section (a)(2), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>39</sup> 16 U.S.C. § 824o–1, Section (a)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.



Government and industry partners should design emergency orders to protect and restore the reliability of these high-priority grid systems and the customers they serve.

Emergency orders should also reflect broader Federal government strategies to defend critical infrastructure. The U.S. *National Security Strategy*, for example, provides crucial guidance on how the United States will deter attacks on critical systems, and -- if deterrence fails -- defeat the attackers.<sup>40</sup> DOE and its industry partners should design emergency orders to help implement the Strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this strategic design process with two further steps. First, building on the provisions of the FPA and on existing industry plans to prioritize the restoration of power, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement EOs and help defend the nation.

- Communications. The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The Rule on Procedures for Issuance of emergency orders (hereinafter referred to as the ‘GSE Rule’) provides a description of the consultative process that (if practicable) will occur before the Secretary sends such orders.<sup>41</sup> However, the GSE Rule does not address the risk that adversaries will attack the industry-government communications systems necessary to issue orders, monitor their compliance, and defeat adversary attacks. Building secure, survivable communications will be essential to the effective use of emergency orders to protect or restore grid reliability. However, the FPA establishes no requirements or funding to do so. Industry and government partners should consider including secure communications as a crucial component of the overall GSE preparedness effort, lest those potential vulnerabilities be left for adversaries to exploit.

Government and utility leaders will also need to coordinate what they tell the American people when the Secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including EOs for prioritized load shedding, could cut off electricity to many thousands of customers in order to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by pre-planned communications playbooks to address customer concerns.

Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Adversaries will strike the grid to achieve

---

<sup>40</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 13.

<sup>41</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1181.

political benefits, including, potentially, the incitement of public panic and a loss of confidence in U.S. leaders. Building upon existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders, will be essential to provide for unity of messaging against such efforts.

- Waivers and Cost Recovery. Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the Act, FERC-approved reliability standards, or environmental regulations.<sup>42</sup> However, potentially valuable emergency orders will be easier to implement if they include pre-planned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.<sup>43</sup> Industry-government dialog will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader pre-planning needed for the financial challenges that grid security emergencies could create, including the catastrophic loss of power company revenue and the breakdown of company access to emergency loans or other financial instruments.

## **II. THREATS, TRIGGERS, AND CONSULTATIVE OPTIONS FOR DECLARING GRID SECURITY EMERGENCIES**

The Federal Power Act leaves the President substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should also consider seeking consensus on the types of threats that on which the development process should focus, and establish decision criteria and consultative mechanisms to support GSE declarations.

### **A. THREATS THAT CAN TRIGGER GRID SECURITY EMERGENCIES: IMPLICATIONS FOR EO DESIGN**

A broad array of natural and manmade hazards can cause multi-state blackouts, including earthquakes and severe weather events such as hurricanes and ice storms. However, in amending the Federal Power Act, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the “occurrence or imminent danger” of:

- 1) “A malicious act using **electronic communication** or an **electromagnetic pulse**, or a **geomagnetic storm** event, that could disrupt the operation of those electronic devices or

---

<sup>42</sup> These waivers apply unless companies carry out orders and related actions in a “grossly negligent manner.” See: 16 U.S.C. § 824o-1, Section (f)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>43</sup> 16 U.S.C. § 824o-1, Section (b)(6), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;”<sup>44</sup> and

2) “Disruption of the operation of such devices or networks, with significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event;” or

3) “A **direct physical attack** on critical electric infrastructure or on defense critical electric infrastructure;” and

4) “Significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.”<sup>45</sup>

Protecting CEI and DCEI against each of these threats will require different types of emergency orders. The threats will also pose disparate challenges for determining the imminence or occurrence of a grid security emergency, ranging from relatively simple to deeply problematic. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the President faces uncertainties about the likelihood and potential consequences of a GSE.

### **1. Geomagnetic Storms as a Possible Initial Focus**

Emergency orders against geomagnetic disturbances (GMD) will entail fewer design challenges than for cyberattacks and other manmade hazards, and could therefore provide opportunities for relatively rapid progress in strengthening GSE preparedness. GMD events occur when coronal mass ejections on the sun create geomagnetically induced currents (GICs) on the surface of the earth. These currents can damage unprotected transformers and other grid infrastructure. Compared to the other threats that can trigger grid security emergencies, determining that there is an imminent danger of a GMD event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the President decide whether to declare a GSE, and will provide hours of warning before the solar energy begins creating destructive GICs.

Industry and government partners can develop emergency orders that exploit this warning time. For example, the Secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of ground induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.<sup>46</sup>

---

<sup>44</sup> Section II of this paper defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of GSE thresholds.

<sup>45</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>46</sup> Dr. Tony Phillips, “Solar Shield--Protecting the North American Power Grid,” NASA, October 26, 2010, [https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\\_solarshield](https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield). See also: MISO, *Geomagnetic Disturbance Operations Plan* (SO-P-AOP-01 Rev: 1), June 9, 2017, p. 5, <https://www.misoenergy.org/Library/Repository/Procedure/SO-P-AOP-01%20Geomagnetic%20Disturbance%20Operations%20Plan.pdf>.

A strong foundation already exists for drafting such orders. Studies of GMD effects on the power grid have generated a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.<sup>47</sup> Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the Federal Government to ensure that it has the capability to predict and detect space weather events, the ability to communicate these assessments to public and private sector stakeholders, protection and mitigation plans for critical infrastructure, and response and recovery plans for GMD events. The order requires Sector-Specific Agencies to “assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event.”<sup>48</sup> NERC standards also exist for addressing GMD threats. TPL-007-1 – *Transmission System Planned Performance for Geomagnetic Disturbance Events* establishes long-lead GMD planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat (DBT) for GMD events.<sup>49</sup> EOP-010-1 – *Geomagnetic Disturbance Operations* also requires Reliability Coordinators to develop GMD mitigation plans and operating procedures, including specific actions that Transmission Operators must take based on predetermined GMD-related conditions.<sup>50</sup>

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyberattacks and other manmade triggers for grid security emergencies. The sun will not intentionally hide preparations for a GMD event or “prepare the battlefield” by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data utility personnel need to maintain situation awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of CEI and DCEI.

The relative ease of drafting orders for geomagnetic disturbances makes such GMD efforts a prime starting point for industry-government collaboration. The North American Transmission Forum (NATF), in coordination with the ESCC, is already examining opportunities to develop template emergency orders for GMD events. But the greater degree of difficulty associated with

---

<sup>47</sup> See: National Oceanic and Atmospheric Administration, *NOAA Space Weather Scales*, April 2011, [https://www.swpc.noaa.gov/sites/default/files/images/NOAA\\_scales.pdf](https://www.swpc.noaa.gov/sites/default/files/images/NOAA_scales.pdf); Metatech (for Oak Ridge National Laboratory), *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*, January 2010, [https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc\\_meta-r-319.pdf](https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf).

<sup>48</sup> The White House, *Executive Order -- Coordinating Efforts to Prepare the Nation for Space Weather Events*, October 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events>.

<sup>49</sup> NERC, *TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events*, December 2014, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States).

<sup>50</sup> The standard, however, does not explicitly lay out what those predetermined conditions should be. See: NERC, *EOP-010-1 – Geomagnetic Disturbance Operations*, June 2014, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States). For an example of GMD plans, see: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, pp. 69-71.

protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of EOs to counter such threats. Instead, DOE and its industry partners should consider pursuing a multi-track development process: at the same time that they seek rapid progress on emergency orders for GMD, they should *immediately* accelerate the long-lead work that will be required against each of the manmade threats that can trigger grid security emergencies.

## **2. Cyber and Physical Attacks**

This study focuses on supporting the development of EOs to protect and restore grid reliability against cyberattacks. The U.S. *National Security Strategy* highlights the imperative to counter the intensifying cyber threats to the grid and other critical infrastructure. The Strategy warns that the vulnerability of U.S. critical infrastructure to cyberattacks and other threats “means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and communications.” Cyber weapons also “enable adversaries to attempt strategic attacks against the United States – without resorting to nuclear weapons – in ways that could cripple our economy and our ability to deploy our military forces.”<sup>51</sup> An immediate focus for EO development efforts should be to help counter such potentially devastating cyber threats, by designing orders to protect or rapidly restore electric service to military bases and civilian-owned facilities vital to the economy and public health and safety.

This study also examines the development of emergency orders against physical attacks on the grid. Since the carefully coordinated attack against the Metcalf, California substation in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high powered rifles or other weapons.<sup>52</sup> Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

Launching physical attacks would entail risks to the adversary beyond those created by cyberattacks. Blowing up transformers and -- potentially -- killing workers who are transporting replacement equipment would immediately escalate conflict with the United States into open kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries will hide on utility networks, arming and pre-positioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

---

<sup>51</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, pp. 12 and 27, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

<sup>52</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation’s Electricity System: Second Installment of the QER*, January 2017, p. 4-34; NERC, *CIP-014-02: Physical Security*, effective October 2, 2015, <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.



Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk-reward calculus in our favor. If EOs can help power companies protect their systems from physical attacks, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Grid owners and operators are also strengthening their preparedness against combined cyber-physical attacks. Such combined attacks can create synergistic disruptions of the grid beyond those from cyber or physical attacks on their own. For example, as in the response to the cyberattacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.<sup>53</sup> Attacks that physically destroy critical components at those substations or shoot utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

To prepare against such difficult challenges, the largest-scale exercise conducted by NERC and the electricity subsector, GridEx, uses combined cyber-kinetic attacks on power companies in multiple U.S. regions as the exercise's scenario. GridEx also assumes that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging far more difficult than in any past U.S. power outage.

This study adopts a similarly severe threat for analyzing possible EOs. In particular, the study examines how orders can protect or restore grid reliability against the combined use of cyber weapons, kinetic strikes, and information warfare against critical electric infrastructure and defense critical electric infrastructure. Of course, separate types of emergency orders will be required against physical and cyberattacks. Orders to deploy additional armed guards to substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead and accounting for the risk of combined attacks will provide valuable context for the development of physical and cyber EOs, and for the public communications support they will require.

The study does not examine options for developing emergency orders against electromagnetic pulse attacks. EMP threats pose a significant potential risk to the grid, and a growing number of utilities are hardening their critical systems against EMP effects.<sup>54</sup> The Department of Energy's EMP strategy provides a valuable framework approach for managing the risks that EMP threats

---

<sup>53</sup> E-ISAC and SANS-ICS, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, March 2016, p. v.

<sup>54</sup> In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to GMDs. The early-time (E1) component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See: Electric Power Research Institute, *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research* (3002000796), December 2013, pp. 3-3-3-4.

pose to the grid and other energy systems.<sup>55</sup> The Department of Homeland Security’s EMP strategy does the same for a broad range of infrastructure sectors.<sup>56</sup> However, significant research will still be required to understand the combined effects of EMP wave components on grid hardware and system-wide operations, and on cost-effective mitigation options and preparedness planning.<sup>57</sup> As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

## **B. THRESHOLDS FOR DECLARING GRID SECURITY EMERGENCIES**

The President can declare a grid security emergency when there is either imminent danger of an attack or when attacks are already occurring.<sup>58</sup> These two circumstances for declaring a GSE will require distinct, sequential types of emergency orders: 1) pre-attack orders to “raise the gates” against imminent cyber and/or physical strikes; and 2) orders to protect grid reliability once attacks are underway, including measures to prevent the spread of cascading failures across critical and defense critical electric infrastructure. DOE and its partners should also consider developing specialized EOs for a third phase of grid security emergencies: operations to accelerate the restoration of power after adversaries have inflicted major blackouts.

Before attacks occur, pre-emptive orders could help grid owners and operators initiate *conservative operations* to reduce the vulnerability of their systems to attack, increase power reserves, and take other measures to manage the grid instabilities that adversaries may seek to create. Power companies already have extensive experience in employing conservative operations (COs) when hurricanes or other severe weather events are approaching. This experience provides a strong foundation on which to develop COs against cyber and physical attacks. However, determining that attacks are imminent can be vastly more difficult than assessing whether a hurricane will strike, especially if adversaries seek to achieve surprise.

A strong foundation also exists to build emergency orders for attacks that are underway. Most important, BPS entities already have plans and capabilities in place to protect grid reliability when major disturbances occur, and reduce the risk that such disturbances will create cascading failures or other widespread disruptions of electric service.<sup>59</sup> For example, NERC already

---

<sup>55</sup> The Department of Energy has set strategic goals for addressing EMP threats, and created an action plan to meet those goals. Department of Energy, *Electromagnetic Pulse Resilience Action Plan*, January 2017; The FY17 NDAA directed DHS to create a similar strategy, which is currently in draft form. “National Defense Authorization Act for Fiscal Year 2017,” Public Law 114-328, *U.S. Statutes at Large* 130 (2016): pp. 2685-2687; and the Electric Power Research Institute (EPRI) continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs* (3002008999), September 2016.

<sup>56</sup> Department of Homeland Security, *Strategy for Protecting and Preparing the Homeland Against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*, forthcoming (Spring 2018).

<sup>57</sup> Idaho National Laboratory, *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*, January 2016.

<sup>58</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>59</sup> The section that follows examines how NERC’s definition of “Adequate level of Reliability” for the Bulk Power System, including the prevention of cascading failures, can be used to help build design standards for emergency order and thresholds for declaring grid security emergencies. North American Electric Reliability Corporation,

requires transmission operators to be able to shed load (i.e., temporarily curtail or cut off electric service to customers) to mitigate operational emergencies.<sup>60</sup> Emergency orders should be developed for equivalent *extraordinary measures* to protect grid reliability.

A third category of emergency orders will also be valuable if (despite such extraordinary measures) attackers are able to create blackouts that jeopardize public health and safety, the U.S. economy, or national security. Electric industry stakeholders should design EOs to *accelerate restoration* of power to critical electric infrastructure and defense critical electric infrastructure if these blackouts occur. The Secretary could also issue such orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these customers. But lists that identify other national security-related assets, including components of the Defense Industrial Base and transportation infrastructure essential for deploying and sustaining military forces abroad, may be closely held by DOD and not yet included in industry restoration priorities. This study will examine how DOE and its industry partners can leverage existing government schemes for identifying critical facilities to help develop and execute EOs for restoration support, and how that sensitive data can be shared with power companies while remaining protected from adversaries.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, EOs for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are underway. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies “stop the bleeding” from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are underway.<sup>61</sup>

DOE and its partners will need considerable flexibility to deal with overlapping GSE phases in designing, issuing, and implementing executive orders. Nevertheless, being able to “rack and stack” potential orders in terms of when they would be issued and which phases of emergency operations they would support can help facilitate a structured, integrated approach to EO development.

---

“Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013.

<sup>60</sup> North American Electric Reliability Corporation, *EOP-011-1: Emergency Operations*, effective April 1, 2017, R1.2.5, [https://www.nerc.com/\\_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).

<sup>61</sup> In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is full restored to pre-event conditions) as the “New Normal” – characterized by “degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months.” See: North American Electric Reliability Corporation, *Severe Impact Resilience: Considerations and Recommendations*, May 9, 2012, pp. 14 and 16.

## **1. Determining When Attacks are Imminent: Criteria for Declaring GSEs and Issuing Emergency Orders**

The Federal Power Act defines GSEs as occurring when attacks that are imminent or underway “could disrupt the operation” of devices or networks that are “essential to the reliability of critical electric infrastructure or defense critical electric infrastructure.”<sup>62</sup> But the Act does not define imminent. Nor does it clarify the degree of potential disruption that will trigger the declaration of a GSE or detail the criteria that the President should use to make such a decision.

In key respects, the BPS system is under cyberattack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant APTs on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS systems, secrete malware designed to disrupt grid operations, and conduct other malicious activity to prepare for possible attacks on critical system components.<sup>63</sup> PJM Interconnection’s former CEO, Terry Boston, said the RTO experiences 3,000-4,000 hacking attempts *every month*.<sup>64</sup> Penetration efforts on a similarly massive scale are likely to be occurring against BPS entities across the United States. And, as in the case of Black Energy and other adversary campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.<sup>65</sup>

The President could conceivably decide that such campaigns constitute “occurring” attacks under the FPA that should trigger the declaration of a grid security emergency (and, presumably, the use of appropriate countermeasures against the perpetrator). Alternatively, the President might take these measures as evidence that there is “imminent danger” of an attack, and declare a GSE before adversaries used embedded malware to disrupt the operation of devices or networks essential to the reliability of CEI or DCEI.

Federal decision makers could also decide to set the threshold much higher. For example, the President might only declare a grid security emergency if adversaries were poised to disrupt CEI and DCEI across multiple regions of the United States, and could sustain those disruptions for a week or more. The text of the Federal Power Act leaves substantial ambiguity over the criteria that should trigger a GSE and justify the issuance of issue emergency orders to protect grid

---

<sup>62</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>63</sup> “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Readiness Team*, March 15, 2018, <https://www.us-cert.gov/ncas/alerts/TA18-074A>; “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Response Team (US-CERT)*, October 20, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-293A>; Defense Science Board, *Task Force on Cyber Deterrence*, February 2017, p. 4; ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*, June 2016, p. 19.

<sup>64</sup> Jon Dougherty, “Biggest U.S. power grid operator suffers thousands of attempted cyber attacks per month,” *Forward Observer*, August 22, 2017, <https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/>.

<sup>65</sup> Black Energy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of Black Energy inflicted the 2016 blackout on Ukraine. Alert (ICS-ALERT-14-281-01E), “*Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*, last updated December 9, 2016, <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.

reliability. In an intense crisis, this ambiguity could fuel disagreements amongst the President's advisors as to whether the threat of attack was sufficiently severe to declare a GSE, and unleash the firestorm of media speculation and congressional concern that a public declaration would produce.

But it would be a mistake to adopt a rigid set of GSE thresholds. Preserving broad latitude for the President to determine what constitutes a GSE will provide flexibility to deal with unforeseen circumstances and help avoid locking U.S. crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicly draw explicit "red lines" that would trigger a GSE. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay U.S. defensive measures, including the issuance of emergency orders to protect grid reliability. Adversaries might even seek to "spoof" the President into declaring a GSE when they had no intention of launching an attack – especially if doing so might incite public panic that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events which emergency orders should be designed to help counter. One option for clarifying such thresholds is to focus on the geographic scope of an emergency. In responding to DOE's *Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance*,<sup>66</sup> the ISO-RTO Council proposed that the use of emergency orders "should be reserved for true widespread emergencies." Equivalent criteria might be created by the President's advisors to support internal deliberations on whether to declare a GSE. However, additional options exist to assist such decision making in ways that are better attuned to the purposes of the Federal Power Act and offer more direct value for developing emergency orders.

## **2. Preventing Cascading Blackouts, Uncontrolled Separation, and other Disruptions of "Adequate Levels of Reliability"**

The North American Electric Reliability Corporation (NERC) has carefully defined what constitutes adequate reliability for the power grid, and the types of large-scale failures in reliability that owners and operators need to prevent. The imminent danger or occurrence of such failures should almost certainly be considered sufficient to declare a grid security emergency. The technical and operational requirements needed to prevent these failures also provide an opportunity to tailor emergency orders for each of them.

The 2003 Northeast blackout spurred efforts to define an adequate level of reliability for the grid and the system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over major portions of the United States, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The

---

<sup>66</sup> Theodore J. Paradise et al., "ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance—RIN 1901–AB40," *ISO-RTO Council*, February 6, 2017, [http://www.isorto.org/Documents/Report/20170206\\_Final\\_IRC-DOE\\_NOPR\\_Comments\\_re\\_Grid\\_Security\\_Emergency.pdf](http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf).



2005 amendments required FERC to certify an Electric Reliability Organization (ERO), which will have “the ability to develop and enforce ... reliability standards that provide for an adequate level of reliability of the bulk-power system.”<sup>67</sup> However, the EPA never defined “adequate level of reliability” (ALR); that task was left to the ERO to complete.

When NERC became the ERO in 2006, defining the ALR became one of its first initiatives. NERC’s Board of Trustees approved an initial definition for the “characteristics of a system with an adequate level of reliability” in 2008.<sup>68</sup> In May 2013, NERC released an updated ALR definition.<sup>69</sup> Three components of NERC’s definition are especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS, and to clarify the scale and scope of threats that EOs should be designed to counter.

The sections that follow examine each of these three components and the failures in reliability they can entail. However, in severe events, all three types of failures often occur in rapid succession and are inextricably linked. Protecting against their combined effects will be a key challenge in preparing for grid security emergencies.

**a. Instability.** NERC defines system instability as “the inability of the Transmission system to remain in synchronism ... characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES.”<sup>70</sup> The BES can experience frequency, voltage, or angular instability – though none should occur during normal operating conditions.<sup>71</sup>

Temporary instabilities occur occasionally; grid protection systems and operational protocols typically protect the bulk power system, mitigating their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, if BES generators accelerate or decelerate too much during a disturbance, the Transmission system may experience large power swings, causing transmission lines to trip and/or generators to go out of step and trip offline, resulting in further acceleration and deceleration.<sup>72</sup> Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread, cascading failures across CEI and DCEI. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur, given the speed at which instabilities propagate. Though difficult to predict, the determination that attackers were poised to both create instabilities and

---

<sup>67</sup> *Ibid.*

<sup>68</sup> North American Electric Reliability Corporation, *Technical Report Supporting Definition of Adequate Level of Reliability*, March 26, 2013, p. 17.

<sup>69</sup> The document refers to the Bulk Electric System (BES) rather than the Bulk Power System (BPS). See note 25 on differences between NERC’s BES and BPS definitions. Again, for the sake of clarity and consistency with the FPA this study uses the term BPS throughout.

<sup>70</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, p. 6.

<sup>71</sup> *Ibid.*, at pp. 1-2.

<sup>72</sup> *Ibid.*, at 6.

nullify protective systems could provide an additional basis for declaring a grid security emergency. Industry and government partners should explore the development of emergency orders for conservative operations to give the Transmission system extra “slack” to (ideally) avoid instabilities, as well as for extraordinary measures to help the system remain in synchronism should major instabilities occur.

**b. Cascading Failures.** NERC defines cascading as “the uncontrolled successive loss of system elements triggered by an incident at any location.” Such cascading “results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.”<sup>73</sup> NERC’s definition of the Adequate Level of Reliability (ALR) for the BPS states that the system will not experience cascading when struck by lightning strikes and other frequent, predictable incidents (i.e., “predefined Disturbances”). But more severe events have caused instabilities which led to cascading in the past and may do so again – especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout was especially wide-ranging and spurred the development of mandatory reliability standards to reduce the risk of such failures in the future. That blackout (which affected approximately 50 million people across the U.S. and Canada) started with a relatively minor incident. On a hot day in August, multiple 345-kV transmission lines tripped after sagging into overgrown trees. While operator actions might have been able to handle such a contingency with proper situational awareness, failures in the utility’s control room alarm processor resulted in operators being unaware of the problem entirely. In an extremely unfortunate coincidence, the utility’s Reliability Coordinator also had computer problems and was lacking the visual tools necessary to provide support.<sup>74</sup> These failures shifted power flows to a system of 138-kV lines which were unable to handle the added current flows, also overloading the last remaining 345-kV path into the area, and beginning the major, uncontrollable cascading sequence.<sup>75</sup> This sequence tripped over 500 generating units and 400 transmission lines in only eight minutes – most of which actually occurred *in the last 12 seconds* of the cascade.<sup>76</sup>

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversary attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying key generation and transmission nodes; altering protective relay settings so that grid components trip off line (or fail to do so) in ways that intensify the outages; denying grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and taking other measures designed to produce cascading failures.<sup>77</sup>

---

<sup>73</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, pp. 1 and 7.

<sup>74</sup> North American Electric Reliability Corporation, *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?*, July 13, 2014, pp. 27-28.

<sup>75</sup> *Ibid.*

<sup>76</sup> North American Electric Reliability Corporation, *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?*, July 13, 2014, p. 109.

<sup>77</sup> Anton Cherepanov and Robert Lipovsky, “Industroyer: Biggest threat to industrial control systems since Stuxnet,” *ESET Blog: WeLiveSecurity*, June 12, 2017, <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat->

Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe – particularly by undermining situational awareness data and capabilities.

The imminent danger or occurrence of adversary-induced cascading outages could be criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt the operation of grid devices and networks essential to CEI and DCEI – and do so on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

As will be discussed in Section III, it may be difficult to determine that an impending attack poses an imminent danger of creating cascading failures given the technical challenges of predicting the systemic effects of cyber and physical strikes. Waiting until an attack is underway to assess the risks of cascades will also pose challenges. As in 2003, failures can spread across vast areas in seconds, and adversaries may seek to disrupt grid operators’ situational awareness. Nevertheless, given the threat that cascading blackouts would pose to CEI and DCEI, any significant risk that adversaries are poised to create such effects should be sufficient to declare a grid security emergency.

Promising opportunities also exist to develop emergency orders to reduce the risk of cascading failures. Emergency load shedding provides one such opportunity. After action reports from the 2003 blackout found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. In particular, a U.S.-Canada task force found that “Timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio.”<sup>78</sup> In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.<sup>79</sup>

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for Transmission Operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation on which to build emergency orders to reduce the risk that physical and cyberattacks will create cascading blackouts, and – potentially – tailor EOs and implementation plans to exclude vital facilities from load shedding.

---

industrial-control-systems-since-stuxnet/; Chris Sistrunk, “ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One),” *SANS Industrial Control Systems*, January 8, 2016, <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>; *United States Computer Emergency Readiness Team*, “Alert (TA17-163A): CrashOverride Malware,” June 12, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-163A>; Dragos, Inc, *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*, June 13, 2017, p. 24.

<sup>78</sup> U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 147.

<sup>79</sup> *Ibid.*, at p. 77.

**c. Uncontrolled Separation.** NERC defines uncontrolled separation as “the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss.”<sup>80</sup> Severe events “resulting in the removal of two or more BES elements with high potential to cascade” can produce uncontrolled separation.<sup>81</sup>

Uncontrolled separation almost always occurs following cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands which “quickly became unstable after the massive transient swings and system separation” because there was insufficient generation within the island to meet electricity demand.<sup>82</sup> Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.<sup>83</sup> In the 1982 West Coast blackout, loss of 500-kV lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, and separation of the system into four unplanned islands.<sup>84</sup> A similar blackout in the same region in 1996 triggered by multiple major transmission line outages, the Western Interconnection again separated into four electrical islands “with significant loss of load and generation.”<sup>85</sup>

Unplanned islands are inherently unstable. Uncontrolled separation only rarely (and near-miraculously) produces synchronous islands in which load and generation are balanced within their perimeters.<sup>86</sup> A better way to produce stable islands may be to pre-plan for them. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, pre-planned islands might become a hedge against cascading failures and uncontrolled separation. In practice, such islanding will entail immense technical and operational problems. Section IV provides a detailed analysis of these opportunities and challenges.

Taken together, these criteria for maintaining grid reliability could constitute “high level” thresholds for declaring GSEs. If the Bulk Power System faced an imminent threat of cascading blackouts, uncontrolled separation, or widespread instability, the potential consequences for the U.S. economy and national security would be so severe that declaration of a GSE should be near-automatic.

However, systemic threats to grid reliability are far from the only criteria that the President might want to consider. Much more narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security – including the National Capital Region – might be

---

<sup>80</sup> North American Electric Reliability Corporation, “Informational Filing on the Definition of Adequate Level of Reliability,” *Filing to the Federal Energy Regulatory Commission*, May 10, 2013, p. 6.

<sup>81</sup> *Ibid.*, at p. 13.

<sup>82</sup> U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 75.

<sup>83</sup> *Ibid.*, at p. 104.

<sup>84</sup> *Ibid.*, at p. 105.

<sup>85</sup> *Ibid.*, at p. 106.

<sup>86</sup> National Academy of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation’s Electricity System* (Washington D.C.: The National Academies Press, 2017), p. 81.

sufficient to declare a grid security emergency. The President should retain adequate flexibility to make such declaration across a broad range of contingencies. Developing emergency orders to protect and restore service to such critical areas should be a priority as well, together with orders to prevent cascading failures across larger portions of the United States.

### **3. Further Options to Support GSE Declarations: Attack Consequences, Geopolitical Circumstances, and Adversary Efforts to “Prepare the Battlefield”**

Additional criteria can help clarify thresholds for declaring GSEs and for issuing emergency orders while providing such latitude. One criterion is the potential impact of attacks on U.S. national security, the economy, and public health and safety. As noted above, the FPA defined GSEs as occurring when attacks “could disrupt the operation” of CEI or DCEI.<sup>87</sup> Policymakers should consider refining that overly broad standard by leveraging the definition of “significant cyber incidents” in Presidential Policy Directive-41 (PPD-41), *United States Cyber Incident Coordination*. Under PPD-41, “significant cyber incident” are those that are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.”<sup>88</sup> That demonstrable harm standard can help set an appropriately high bar for declaring GSEs and issuing EOs

For determining that attacks are imminent, decision makers might also take the geopolitical climate into account. It is (barely) conceivable that adversaries will launch a “bolt from the blue” attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region, and attack the grid to disrupt the deployment of U.S. forces to the region or achieve other military and political goals.<sup>89</sup> Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause demonstrable harm via grid attacks, should carry greater weight in crises than in peacetime.

The emergence of a regional crisis would also provide opportunities to intensify and specially target searches for destructive malware. Industry and government should ensure that as tensions rise, agencies are already prepared to ramp up intelligence sharing with BPS entities, especially in terms of specific malware signatures to search for in utility networks, data logs, and critical equipment. Pre-attack emergency orders could help facilitate such intensified collaboration.

Gathering and sharing data on adversary efforts to prepare the battlefield can also support GSE determinations. DOE and its industry partners have taken major strides to improve such sharing;

---

<sup>87</sup> 16 U.S.C. § 824o–1, Section (a)(7), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

<sup>88</sup> White House, *Presidential Policy Directive - United States Cyber Incident Coordination*, July 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

<sup>89</sup> Section II C examines these national security-related issues and their implications for designing emergency orders.



especially on the operational technology networks (OT) and other systems that help control grid operations. For example, DOE's Cybersecurity Risk Information Sharing Program is a public-private partnership to build bi-directional situational awareness and facilitate classified and unclassified information sharing.<sup>90</sup> The CRISP is managed by the E-ISAC, which plays an integral role in establishing situational awareness in the electricity subsector. The E-ISAC is also central to electric industry incident coordination efforts, including cybersecurity threat assessments and sharing incident data.<sup>91</sup>

Advancing the ability to improve situational awareness of OT networks is a key focus of DOE's current activities. The Department is currently in the early stages of taking the lessons learned from CRISP and developing an analogous capability to monitor traffic on OT networks via the Cybersecurity for the Operational Technology Environment (CYOTE) pilot project. Observing anomalous traffic on networks – and having the ability to store and retrieve network traffic from the recent past – can be the first step in stopping an attack in its early stages.

The President's advisors may want to employ additional technical criteria in making pre-attack GSE determinations. One opportunity lies in using the Industrial Control System (ICS) Cyber Kill Chain, which identifies the specific, sequenced phases that adversaries execute in order to conduct attacks that inflict predictable physical effects on grid equipment and operations.<sup>92</sup> Stage 1 begins with planning and reconnaissance against ICS networks, and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing capabilities to attack ICS networks, and – ultimately – executes the attack. Evidence of an adversary's position along this Kill Chain could help support decision-making on the imminence of potential threats, with the final phases posing the most proximate risks of attack.

Another option lies in using established Federal cyber incident criteria. For example, consistent with PPD-41, *United States Cyber Incident Coordination* (July 2016), the National Cyber Incident Response Plan (NCIRP) issued in December 2016 provides a Cyber Incident Severity Schema to serve as “a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments” and agencies.<sup>93</sup> Appendix A provides the Schema. As efforts go forward to refine the Schema and the NCIRP, significant opportunities will exist to crosswalk and provide for consistency between such Federal Government-wide assessment systems and possible GSE thresholds for internal use by the President and supporting staff and departments.<sup>94</sup>

---

<sup>90</sup> “Energy Sector Cybersecurity Preparedness,” *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

<sup>91</sup> “Electricity ISAC,” *NERC*, n.d.a., <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>92</sup> The ICS Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin in 2011 to “help the decision-making process for better detecting and responding to adversary intrusions.” The ICS Cyber Kill Chain tailors that decision-making tool for ICS-specific cyber threats and consequences. See: Michael Assante and Robert M. Lee, “The Industrial Control System Cyber Kill Chain,” *SANS Institute*, <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.

<sup>93</sup> Department of Homeland Security, *National Cyber Incident Response Plan*, December 2016, pp. 29-30.

<sup>94</sup> One option would be to explicitly link the declaration of a GSE to the designation of a cyber incident as a “Level 5 Emergency,” which poses “an imminent that to the provision of wide-scale critical infrastructure services, national government stability, or to the lives of U.S. persons.” But other Schema levels (either lower, or, potentially, higher if

Of course, an enormous difference exists between making preparations for an attack and actually launching one. But if adversaries were to suddenly move to the penultimate phase of stage 2 (delivery and installation of the attack capability) during an intense political crisis or regional confrontation, evidence that they had taken such a move could help support GSE decision-making. Gathering such evidence against sophisticated attackers may require sustained improvements in sensors and OT/IT system monitoring.

### **C. PRE-ATTACK GSE DECLARATIONS: OPTIONS FOR DATA SHARING AND CONSULTATION WITH INDUSTRY**

Decisions regarding pre-attack GSE declarations would benefit significantly from thorough industry consultation. However, neither the Federal Power Act nor the *Final Rule on Grid Security Emergency Orders: Procedures for Issuance* explicitly provide for such discussions. The GSE Rule specifies that “before an emergency order is put into effect and, to the extent practicable and in light of the nature of the grid security emergency and the urgency of the need for action, efforts will be made to consult” with the ESCC, the owners, users and operators of CEI and DCEI, and other resilience stakeholders.<sup>95</sup> DOE might benefit from making equivalent commitments to seek industry input on the declaration of GSEs.

Only power companies will have access to the precursory malware that adversaries implant on their networks, as well as unique expertise in assessing the potential impact of the malware on their systems if attacks begin. Government leaders should consider consulting with BPS entities before the President declares a GSE so that the President’s advisors can benefit from their technical perspectives, and so that government and industry can jointly prepare for the media turmoil that a declaration will almost certainly produce.

As with consultations on issuing orders, urgent circumstances could foreshorten or preclude opportunities for government dialog with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of “bolt from the blue” attacks. However, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be extraordinarily valuable in determining whether (and when) to declare a grid security emergency. Now is the time to explore options to coordinate such discussions, preferably by leveraging existing consultative mechanisms under the ESCC and E-ISAC.

### **III. A FRAMEWORK FOR DEVELOPING EMERGENCY ORDERS: GSE PHASES AND ORDER DESIGN OPTIONS**

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal with these ambiguities is to delay the

---

additional categories are developed) could provide for such linkages. Department of Homeland Security, *National Cyber Incident Response Plan*, December 2016, p. 38.

<sup>95</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1181.

declaration of a GSE until blackouts begin, foregoing the benefits of issuing pre-attack emergency orders. Industry and government partners should instead explore options to design EOs for the Secretary to issue when risks of cyberattack are elevated – especially if such orders will have little or no disruptive effects on normal grid service. These partners should also develop more extreme and potentially disruptive options for use when attacks are underway and when restoration operations begin.

## **1. Pre-Attack Options**

Conservative operations that utilities implement against natural hazards help illuminate the value that pre-attack EOs could offer against manmade threats. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects, and prepare for possible response and restoration operations if grid infrastructure is damaged.<sup>96</sup> For example, Reliability Coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.<sup>97</sup> Power companies may also cancel non-critical generation and transmission maintenance activities and staff their back-up control centers, critical BPS substations, and other key facilities to set the stage for emergency operations as hurricanes approach.<sup>98</sup>

A key feature of these frequently-used conservative operations (COs) is that they do not disrupt normal service to customers. The negligible impact of these COs on day-to-day service helps make them more viable for a utility to implement when the storm's path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the U.S. coast. Instead, they provide a wide “cone of uncertainty” that becomes increasingly narrow as the hurricane approaches. However, utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other COs. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these COs do not affect normal service to customers enhances the willingness of utility leaders to order their implementation amidst the uncertainty.

---

<sup>96</sup> Conservative operations are not defined in the NERC Glossary of Terms. However, many Reliability Coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken “to implement additional actions to ensure the BES [Bulk Electric System] remains reliable in the face of the additional threats” when “events, conditions, or circumstances may put the [BES] at an increased level of risk, compared to normal operating conditions.” See: PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 3, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>. Similarly, the Western Electricity Coordinating Council, defines Conservative Systems Operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets “Are restricted and managed in order to maintain or the restore reliability of the power system from the negative influence of a triggering event or condition.” See: Western Electricity Coordinating Council, *Conservative System Operations* (training slides, n.d.a.), p. 4, [https://www.wecc.biz/Administrative/ProviderXXX\\_CSO\\_20XX\\_Presentation.pdf](https://www.wecc.biz/Administrative/ProviderXXX_CSO_20XX_Presentation.pdf).

<sup>97</sup> PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 3, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.

<sup>98</sup> PJM, *Conservative Operations* (training materials presented on January 27, 2015), p. 9, <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.

Industry and government partners should borrow from this model to develop orders for pre-attack conservative operations against cyber and/or physical attacks. As a regional confrontation or other precipitating crisis intensifies, it is possible (though unlikely) that the U.S. intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. Instead, based on evidence gathered on utility networks and other sources, the President may need to declare a GSE when it is still not certain that an attack will occur, in order to ensure that sufficient time exists to implement pre-attack conservative operations.

As with COs that power companies adopt when they are within a hurricane's cone of uncertainty, it will be especially helpful to develop pre-attack emergency orders that will not disrupt day-to-day electric service. If the Secretary issues such orders for BPS entities to adopt COs and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented them – but only if those orders also enable entities to recover the costs of doing so. Section IV of this study examines possible “no regrets” emergency orders for conservative operations. Many of them could order COs similar to those developed for natural hazards. For example, pre-attack EOs might order BPS entities to increase generation reserves and/or re-dispatch resources out of least cost operations, and reimburse those entities for the costs they incur.

Other orders might be threat-specific: i.e., to intensify scrutiny of OT networks for malware. Power companies could implement all such no regrets EOs without cutting off power to customers or creating grid instabilities. DOE and its industry partners must consider the development of such options as a special priority for follow-on engineering and operational analysis. Appendix B contains a preliminary list of options for conservative operations which builds on current utility conservative operations procedures, and adds additional, adversary-specific options.

## **2. Putting Additional “Arrows in the Quiver:” Possible EOs for Extraordinary Circumstances**

Industry and government partners should also develop emergency orders that could offer additional benefits for protecting or restoring reliability, even at the price of disrupting normal electric service. Most such orders would be used only under extraordinary circumstances: that is, when adversaries were poised to cripple the reliable operation of the grid, and the BPS was at severe risk of instability, uncontrolled separation, or cascading failure.<sup>99</sup>

Emergency actions taken against severe natural hazards again exemplify the benefits of developing extraordinary measures for grid security emergencies. The shutdown of grid infrastructure on warning of catastrophic storm surges offers a case in point. During Superstorm Sandy, Consolidated Edison (Con Ed) faced the risk of having critical substations and underground electrical equipment inundated by the worst storm surge in nearly 200 years. If seawater hits systems that are still carrying electricity, catastrophic physical damage will result for transformers and other difficult-to-replace grid components. Consolidated Edison's team

---

<sup>99</sup> This formulation follows the definition of reliable operation in FPA, section 215, 16 U.S. Code § 824o(a)(4).

made the politically difficult decision to prevent such damage by pre-emptively cutting of power to lower Manhattan. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.<sup>100</sup> Moreover, Con Ed limited the disruptiveness of the shutdown by notifying customers hours earlier that the utility might halt service, and by already having plans in place to prioritize the restoration of service to hospitals, water-pumping stations, and other critical facilities.<sup>101</sup>

BPS entities continue to use “shutdown on warning” as an effective tool to avoid equipment damage against severe weather, and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent damage to equipment and speed restoration. Generation owners similarly chose to shut down or evacuated some generating units in the storm’s projected path.<sup>102</sup>

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and HVAC systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

Extraordinary measures designed for cyber and physical attacks may entail even greater risks and uncertainties. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an attack is likely to cause cascading failures and demonstrable harm to the U.S. economy, national security, and/or public health and safety. The potential impact of APTs on reliable grid operations may be difficult to determine until attacks are well underway. Even then, myriad factors (including many that grid operators can influence) will affect the likelihood and scope of potential cascading failures.

Nevertheless, a range of emergency orders could help BPS entities reduce the risk of cascading failures and accelerate the restoration of power if outages occur. These EOs vary in terms of when the Secretary would issue them: 1) when attacks are imminent; 2) when they are underway; and 3) when major blackouts exist, and utilities must prioritize and accelerate power restoration to prevent demonstrable, and potentially catastrophic, harm to public safety, national security, and the economy.

Emergency orders can also vary in terms of the degree of disruption they would inflict on normal electric service (and, in many instances, the specific threats they will be designed to counter). Some EOs, including no regrets orders, will have little or no disruptive impact. Others would

---

<sup>100</sup> Rich Miller, “Con Edison Shuts Off Power in Lower Manhattan,” *DataCenter Knowledge*, October 29, 2012, <http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutdown>.

<sup>101</sup> Scott DiSavino and David Sheppard, “ConEd cuts power to part of Lower Manhattan due to Sandy,” *Reuters*, October 29, 2012, <https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030>.

<sup>102</sup> North American Electric Reliability Corporation, *Hurricane Harvey Event Analysis Report*, March 2018, p. v.



have massive effects but – as in cutting off power during Sandy – would also protect grid reliability against longer term disruption and accelerate the prioritized restoration of power.

Figure 1 illustrates these different categories and examples of possible EOs that would fall within them. The leftmost column includes possible EOs that the Secretary would issue when attacks are imminent. Orders for conservative operations, especially those in the no regrets category, would fall into the lower spectrum of disruption to normal service.

**Figure 1 – Emergency Order Matrix: Examples of EO Designs**

Disruption of Normal Grid Reliability / Service	High	Pre-Planned Islanding	Prioritized Load Shedding	Movement of In-Service Transformers to Higher Priority Locations
	Low	Conservative Operations	Suspension of Wholesale Market Operations	Transportation Support for Replacement Transformers
		Protect Reliability When Attack is Imminent	Protect Reliability When Attack is Underway	Restore Service/Reliability
Grid Security Emergency Response Phase				

***a. Extraordinary Measures for Pre-Attack Protection of Grid Reliability: Islanding as a (Problematic) Example***

Pre-attack options with greater disruptive effects would populate the upper left box. Pre-planned power islanding offers an “in extremis” option that has garnered especially strong industry and government interest over the past few years. Microgrids provide the most familiar type of power island. A growing number of military installations (and a handful of hospitals and universities) have generators and other electric infrastructure on their bases, configured so that if the surrounding grid is at risk of losing power, the installations can separate themselves from the grid and operate independently as a power island.

Microgrids do not offer a “bulletproof,” all-purpose defense against imminent attacks. Cyber adversaries are sure to treat on-base electric infrastructure (including renewable generation assets and other systems) as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas-fired generators, the power they provide is only as resilient as

the gas transmission and distribution systems that supply them -- and cyber threats to natural gas systems are rapidly escalating.<sup>103</sup> Moreover, building microgrids requires extensive investment in grid infrastructure – especially if bases want to provide power not only to critical loads within their perimeters, but also for the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to traditional microgrids, power companies have also explored other means of establishing power islands when severe disruptions are imminent. Participants of GridEx, the electric industry’s premier exercise series, have extensively discussed one option that provides an especially useful basis for developing possible pre-attack emergency orders. GridEx participants note that it might be possible to pre-plan to establish large power islands by using existing grid infrastructure within their boundaries. On warning of an imminent attack or under other extraordinary circumstances, power companies would separate the power island from the surrounding grid and operate independently to serve the critical loads within it.

However, strategic islanding will only be practical if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for pre-planned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands. Moreover, standing up islands would severely disrupt day-to-day service for non-critical customers, and create instabilities for surrounding systems that could produce additional service disruptions, economic disruption, and societal unrest. Accordingly, strategic islanding might be considered a “huge regrets” emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created. Further studies will need to examine different models for pre-planned islanding, examines the design and operational challenges they would entail, and analyzes additional pre-attack options for emergency orders.

### ***b. Extraordinary Measures when Attacks are Occurring***

Emergency orders for attacks that are underway could entail similar variation in the degree to which they will disrupt normal service. The lower box in the center column of Figure 1 provides an example of a low-disruption emergency order: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate, “real time” needs or for the next day). These entities have taken extensive measures to keep these market functions separate from their operational control of the grid. Nevertheless, cyberattacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, crush the valuation of power companies on Wall Street, and magnify the damage to the U.S. economy that attacks on the grid will create.

---

<sup>103</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation’s Electricity System: Second Installment of the QER*, January 2017, p. 7-7; Paul W. Parfomak, “Pipelines: Securing the Veins of the American Economy,” *Testimony Before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*, April 19, 2016, pp. 2-3, <http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf>.

RTOs are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the Transmission Operator<sup>104</sup> for the Mid-Atlantic and other U.S. regions, has called for the development of mechanisms to permit “non-market” operations in extreme circumstances.<sup>105</sup> A number of options exist to provide for such operations. For example, if the Secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell power at a fixed price pre-determined by DOE.<sup>106</sup> Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high benefit/low disruption emergency orders examined later in this study, including orders for maximum power generation when attacks are underway, will also fall into this category.<sup>107</sup>

Utilities are already beginning to develop tools and procedures to support extraordinary operations, which DOE and industry can leverage in EO development efforts. The ESCC, for example, has led a focus on exploring how entities may operate the grid “under sub-optimal circumstances,” to ensure that these entities can anticipate, plan for, and practice using extraordinary measures to do so.<sup>108</sup> Notably, this includes the North American Transmission Forum’s “Spare Tire” program, launched in 2016, which is exploring how entities may operate the BES without primary and backup control centers.<sup>109</sup>

---

<sup>104</sup> The NERC Glossary defines Transmission Operator as: “The entity responsible for the reliability of its local transmission system, and that operates or directs the operations of the transmission Facilities.” Transmission Operator Area is defined as: “The collection of Transmission assets over which the Transmission Operator is responsible for operating.” See: “Glossary of Terms Used in NERC Reliability Standards,” NERC, last updated January 31, 2018, [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).

<sup>105</sup> PJM Interconnection, LLC, “COMMENTS AND RESPONSES OF PJM INTERCONNECTION, L.L.C.,” *In Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000), March 9, 2018, pp. 6 and 39-40.

<sup>106</sup> Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. *Ibid.*, at p. 39.

<sup>107</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See: PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see: MISO, “MISO January 17-18 Maximum Generation Event Overview” (slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018), <https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf>.

<sup>108</sup> “ESCC,” *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.

<sup>109</sup> “North American Transmission Forum External Newsletter,” *North American Transmission Forum*, January 2018, <https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf>. For more information on NATF’s Spare Tire program, see: North American Transmission Forum, *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—a Spare Tire Approach*, 2017, <http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf>.

Industry and government partners will also need to develop more disruptive EOs that can protect grid reliability in extraordinary circumstances. The top center box of Figure 1 provides a case in point: prioritized load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by shedding load – most often by implementing rotating blackouts.<sup>110</sup>

Grid operators used load shedding to protect grid reliability during the “Big Chill” that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT initiated controlled rolling blackouts during the event that affected a total of 4.4 million customers over the course of the event.<sup>111</sup> Those temporary blackouts were no doubt disruptive, especially for customers with electric heating systems. However, by reducing the risk of cascading failures, load shedding offered compelling system-wide benefits for protecting reliability.

Industry and government partners could develop emergency orders for load shedding to protect grid reliability during cyber and/or physical attacks. If adversaries are able to inflict deep, multi-region losses in generation and transmission resources, load shedding will offer an essential tool to prevent broader grid instabilities – albeit at the price of disrupting normal service to many millions of customers. NERC already requires BPS entities to have plans for load shedding.<sup>112</sup> In the EO design process, industry and government can build on that foundation to not only protect against cascading failures, but also prioritize load shedding so as to sustain service to facilities critical for national security, the economy, and public health and safety.

### ***c. Emergency Orders to Support Power Restoration***

The rightmost column in Figure 1 provides the third category for emergency orders: EOs that can help grid owners and operators restore power after widespread outages occur. In past cascading failures of the U.S. electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days or less because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators,

---

<sup>110</sup> North American Electricity Reliability Corporation, *Severe Impact Resilience: Considerations and Recommendations*, May 9, 2012, p. 11.

<sup>111</sup> FERC and NERC, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*, January 2016, p. 61.

<sup>112</sup> NERC standards currently emphasize automatic load shedding to protect grid reliability. See: NERC, *PRC-006-3 – Automatic Underfrequency Load Shedding*, effective October 1, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States); and NERC, *PRC-010-2 – Under Voltage Load Shedding*, effective April 2, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States). However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing EOs to prevent or mitigate cascading failures. See: NERC, *EOP-011-1 Emergency Operations*, effective April 1, 2017, [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).

transmission lines, and other system components are designed to trip off line when instabilities occur, thereby protecting them from being damaged by power surges – and leaving them available to help rapidly re-establish the flow of power.<sup>113</sup>

However, if cyber or physical attacks destroy transformers and other critical system infrastructure, requirements to repair or replace such assets could greatly lengthen and complicate restoration operations. BPS entities already have detailed plans to restore power and, as circumstances dictate, prioritize the restoration of service to nuclear power plants and other critical customers. Industry and government should consider developing emergency orders that build on these existing plans and capabilities, and prioritize restoration for a wider array of CEI and DCEI – even if adversaries inflict unprecedented physical damage on grid components.

One option for restoration orders includes ordering utilities to operate in an N-0 operating state, unless one contingency would cause cascading failures. Currently, NERC standards require BPS entities to operate in an N-1 state: they are able to handle the most severe single contingency ('N-1').<sup>114</sup> Operators may be required to shed load to maintain the N-1 state. However, returning to an N-1 state after a major outage is likely to be a lengthy process, involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. If the Secretary were to order utilities to operate at N-0 as needed, they could do so without facing punishment for violating NERC standards. Creating such an option would provide greater operating flexibility and ensure that entities can continue to serve as much load as possible. Entities would only be required to shed load for the most severe single contingency if that single contingency would cause cascading failures or following a contingency that required load shedding to eliminate overloads or low voltage.

Restoration EOs should also account for the risk that adversaries will continue their attacks as power companies begin restoring service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to U.S. military bases and other vital facilities, and seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeted against power restoration operations can help achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply.

The Department of Defense can play a vital role in preventing such attacks. If directed by the President, United States Cyber Command (USCYBERCOM) and other DOD components would do their utmost to “shoot the archer,” and prevent the adversary’s cyber forces from launching further strikes on the grid and other U.S. targets. But re-attacks may nevertheless occur. For example, unless power companies thoroughly scrub advanced persistent threats already hidden

---

<sup>113</sup> NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, December 2010, p. 1. See also: U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 8.

<sup>114</sup> North American Electric Reliability Corporation, *BAL-002-2(i) – Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event*, Requirement R2, effective January 1, 2018.



their networks, those APTs may launch repeated re-attacks against the grid and create recurring outages.<sup>115</sup> Physical attacks to disrupt restoration operations, including against replacement transformers being moved to critical substations, would create additional challenges.<sup>116</sup>

As with EOs for imminent and ongoing attacks, emergency orders to accelerate power restoration will differ in their disruptiveness to normal grid operation. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks and barges) from where power companies store them to where they are needed as replacements.<sup>117</sup> The Secretary has no authority under the Federal Power Act to issue orders to transportation sector assets. However, in collaboration with the Department of Transportation, rail and other asset owners, and SLTT transportation agencies, DOE and the private sector could pre-plan to waive transportation regulations, inspection requirements, and other potential impediments on a nationwide basis. Such plans could also be structured to help protect transportation operations against active shooters or other attacks.

EOs could also be created for *in extremis* restoration operations that would more sharply depart from existing industry plans and procedures. As the starting point for that development process, power companies and their government partners might assume that attacks will not be “one and done,” but instead be part of a sustained campaign in which adversaries will single out restoration operations for disruption. An example of *in extremis* orders: if adversaries managed to damage or destroy an extraordinarily large number of transformers, the Secretary might order that surviving, in-service transformers in the same voltage class be removed from their substation and transported to serve vital national security facilities in the National Capitol Region or other areas. Such orders could create severe disruptions in existing service. However, the benefits might be greater still for helping the United States defeat its adversary.

### **3. Next Steps in the EO Development Process**

Potential emergency orders differ not only in terms of the phases of an attack in which they would be most useful, and in their mix of benefits and disruptive impact on normal grid operations, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create – especially those that fall into the “no regrets” category. As noted above, utilities frequently use COs to help protect grid reliability in severe weather events, and a growing number of companies are already building on that foundation to draft equivalent COs against cyber and physical threats.<sup>118</sup> Emergency orders based on those initiatives constitute “low hanging fruit;” creating such orders offers an immediate opportunity

---

<sup>115</sup> Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee: Part I – Incident Response*, June 2016, p. 7.

<sup>116</sup> The GridEx exercise series accounts for physical attacks that disrupt restoration operations. See: NERC, *Grid Security Exercise: GridEx III Report*, March 2016.

<sup>117</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, pp. 12-13, <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>118</sup> PJM, *PJM Manual 13: Emergency Operations* (Revision 65), January 1, 2018, p. 54.

for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging EO initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are underway, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. The next step to do so is to examine how emergency orders can be framed to reflect and achieve specific U.S. security priorities and meet the other development requirements that they will entail.

#### **IV. ADDITIONAL EMERGENCY ORDER DESIGN PARAMETERS AND SUPPORTING INITIATIVES**

The U.S. *National Security Strategy* provides crucial guidance on how emergency orders can help deter attacks on the grid and other U.S. targets, and how those orders can help the United States defeat adversaries if deterrence fails. However, DOE and BPS entities will also need to overcome the immense communications challenges that the use of emergency orders will entail, including requirements to explain to the U.S. public why extraordinary measures are being employed and what they should expect if attacks continue. Incorporating provisions for regulatory waivers and cost recovery in the design of template emergency orders will offer compelling advantages as well.

##### **A. DETERRING AND DEFEATING U.S. ADVERSARIES**

Adversaries will strike the U.S. grid not merely to cause blackouts, but as a means to help them achieve their broader political, economic, and military objectives against the United States. Government and industry partners should design emergency orders to help prevent attackers from accomplishing their objectives, and – ideally – help deter them from attacking at all.

The U.S. *National Security Strategy* offers an overarching framework to guide such design efforts. The *Strategy* emphasizes that cyber threats to U.S. critical infrastructure are becoming increasingly severe, and notes that cyber weapons “enable adversaries to attempt strategic attacks against the United States – without resorting to nuclear weapons – in ways that could cripple our economy and our ability to deploy our military forces.”<sup>119</sup> To counter these threats, the *Strategy* identifies two essential priorities, both of which emergency orders can be designed to support:

- Deter adversaries from attacking by convincing them they will suffer “swift and costly consequences” and be defeated if they strike the grid or other U.S. targets;<sup>120</sup>
- Strengthen infrastructure resilience to make adversaries doubt that “they can achieve their objectives” if they do attack (i.e. deterrence by denial).<sup>121</sup>

---

<sup>119</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 27.

<sup>120</sup> *Ibid.*, at p. 28.

<sup>121</sup> *Ibid.*, at p. 13.

## **1. Deterrence through Threats of Punishment and Defeat: Implications for Emergency Order Design**

One important way that emergency orders can strengthen deterrence is by helping convince adversaries that the United States will be able to effectively respond to attacks and impose consequences that those adversaries would consider unacceptable. A relatively small number of U.S. military bases are responsible for conducting such response operations. The U.S. Defense Science Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of U.S. strike systems (cyber, nuclear, and non-nuclear) and supporting infrastructure to ensure “that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyberattacks.”<sup>122</sup> Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should and immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which U.S. strike systems rely and ensure that they have reliable power for however long a conflict might continue.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The *Strategy* emphasizes that “We must convince adversaries that we can and will defeat them – not just punish them if they attack the United States.”<sup>123</sup> As noted in Section II, adversaries are most likely to attack the grid in the context of an intense regional confrontation with the United States and its allies in the South China Sea, the Baltics, or some other crisis abroad. A vast array of U.S. Defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy and sustain U.S. power projection forces for regional contingencies. Ensuring the availability of resilient power for these essential facilities and functions will require the development of emergency orders to serve a greatly expanded set of customers than for U.S. strike systems alone, and encompass a much larger array of DCEI owners and operators.

Emergency orders and implementation plans will need to account for a further challenge: the risk that adversaries will selectively target defense critical electric infrastructure and prioritize its disruption through especially sophisticated cyber and physical attacks. The Department of Defense (DOD) *Mission Assurance Strategy* (2012) emphasizes the growing risk that adversaries will seek to degrade U.S. military capabilities by attacking the infrastructure on which DOD depends. In particular, “Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting critical Defense and supporting civilian capabilities and assets,” including the U.S. power grid.<sup>124</sup>

---

<sup>122</sup> James N. Miller and James R. Gosler, “Memorandum for the Chairman, Defense Science Board” (preamble), *Task Force on Cyber Deterrence*, February 28, 2017. See also: Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, pp. 3, 6-7, 11-12, and 17-18.

<sup>123</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 28.

<sup>124</sup> Department of Defense, *Mission Assurance Strategy*, April 2012, p. 1, [http://policy.defense.gov/Portals/11/Documents/MA\\_Strategy\\_Final\\_7May12.pdf](http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf).

Electric companies and Defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds to serve Defense installations provides a valuable means of strengthening resilience.<sup>125</sup> Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.<sup>126</sup> And, as briefly discussed in Section II, utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as “power islands” independent of the surrounding grid.<sup>127</sup>

While valuable, these initiatives do not eliminate the need to develop Defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases. Emergency generators will break down in long duration outages, and resupplying them with fuel will become increasingly difficult at installations that lack massive storage tanks. Large-scale microgrids for islanded operations can provide more resilient power; DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for warfighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, ranging from the water utilities and other “outside the fence” infrastructure that support base operations, to the intermodal transportation systems that help deploy and sustain U.S. forces abroad.

Emergency orders can help support deterrence and power projection far more quickly and with less infrastructure investment. Over the past year, the Department of Defense has been collaborating with power companies and DOE to develop new emergency measures to protect the resilience of electric service to military bases by prioritizing the flow of power to bases when generation capacity falls short of total load, and through other emergency operations. BPS entities are also launching initiatives with DOD and DOE to ensure that power to Defense installations can be restored far more rapidly than is possible today if adversaries create wide-area blackouts.<sup>128</sup>

---

<sup>125</sup> Department of Defense (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment), *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*, July 2017, p. 39, <https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf>.

<sup>126</sup> *Ibid.*, at 40.

<sup>127</sup> *Ibid.* at 39. See also: Lincoln Laboratory, *Microgrid Study: Energy Security for DoD Installations* (Technical Report 1164), June 2012, <https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf>; and Pew Charitable Trusts, *Power Begins at Home: Assured Energy for U.S. Military Bases*, January 12, 2017, pp. 13-15. A number of “islandable” microgrid projects are underway at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See: Michael McGhee, “EEI Executive Advisory Committee,” (slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017), p. 4, [http://www.asaie.army.mil/Public/ES/oei/docs/EEI\\_Exec-Committee.pdf](http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf); and Cheryl Kaften, “DoD Tests Energy Continuity with ‘Islanded’ Microgrid,” *Energy Manager Today*, April 5, 2017, <https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/>.

<sup>128</sup> “Rapid Attack Detection, Isolation and Characterization Systems (RADICS),” *Defense Advanced Research Projects Agency*, n.d.a., <https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems>.

These initiatives provide an increasingly robust foundation for developing emergency orders to reinforce U.S. deterrence and power projection capabilities. For protection against imminent attacks, it may be possible for power companies to develop plans for conservative operations that are specially targeted to protect the defense critical electric infrastructure in their service areas. Pre-planned islanding could provide unique benefits for military bases and supporting systems (though only if power companies can overcome the immense technical and operational impediments such islanding entails). The development of EOs and company-specific implementation plans for prioritized load shedding, in extremis restoration support, and other potential orders also offer additional opportunities to build on industry-government collaboration already underway for post-attack emergency operations.

The prerequisite for these development efforts will be for the Secretary to identify which military bases and supporting assets are most critical to protect. Section 215A of the Federal Power Act provides a starting point to do so. The Act requires the Secretary of Energy, in consultation with other Federal agencies and grid owners and operators, to identify and designate “critical Defense facilities” in the 48 contiguous states and the District of Columbia that are “1) critical to the defense of the United States; and 2) vulnerable to a disruption of electric energy provided to such facility by an external provider.”<sup>129</sup> Congress also created a definition of *Defense Critical Electric Infrastructure* (DCEI) to help guide implementation of that requirement. DCEI constitutes “any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]” as a critical Defense facility, “but is not owned or operated by the owner or operator of such facility.”<sup>130</sup>

The Department of Energy is already working with the Department of Defense to identify and strengthen the resilience of power flows to critical Defense facilities. DOE is also already working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate infrastructure identified as DCEI. Fortunately, DOD already has a well-established, continuously-updated list of Defense Critical Infrastructure (including military bases and other assets) to help provide input to DOE.<sup>131</sup> A wide variety of factors contribute to determining the criticality of a particular military base or other Defense asset. However, for designing emergency orders that help achieve the deterrence and defense priorities of the *National Security Strategy*, priorities for protecting and restoring service fall into three categories. Figure 2 depicts these categories as a set of concentric circles.

## Figure 2 – Categories for Protecting Defense Critical Electric Infrastructure

---

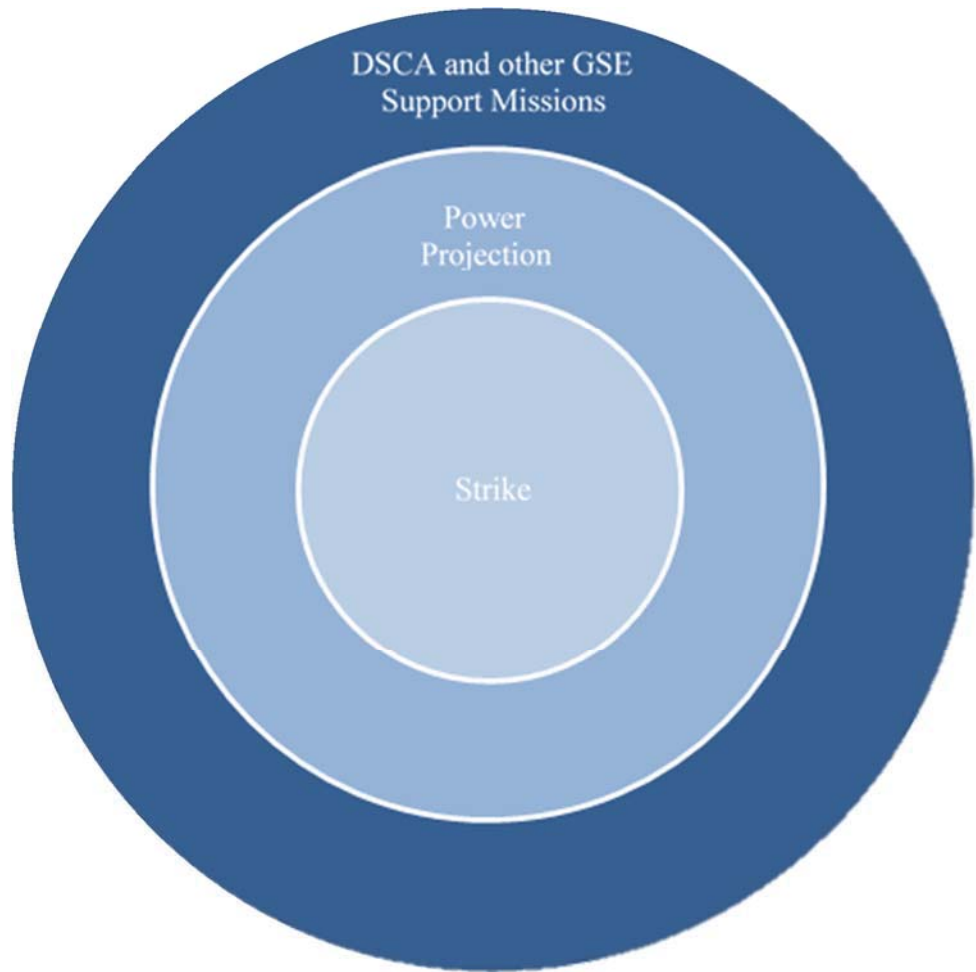
<sup>129</sup> 16 U.S.C. § 824o–1, Section (c), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>130</sup> 16 U.S.C. § 824o–1, Section (a)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>131</sup> See: Department of Defense, *Department of Defense Manual 3020.45: Defense Critical Infrastructure Program (DCIP): Execution Timeline*, last updated May 23, 2017, <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>; and Department of Defense, *Department of Defense Directive 3020.40: Mission Assurance (MA)*, November 29, 2016, [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).



At the innermost core lies those installations and supporting infrastructure that are essential for inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital; protecting the reliability of the DCEI on which they depend is crucial and should be the top priority for developing emergency orders and company-specific implementation plans.



The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining them abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the U.S. grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. The Department of Defense is in the process of identifying the specific facilities and supporting infrastructure that is required to help execute Operational Plans (OPLANS) around the globe.<sup>132</sup> DOD also has well-established criteria and assessment methods to prioritize these supporting assets for risk-mitigation.<sup>133</sup> These tools should be used to identify the broader set of defense critical electric infrastructure needed for deterrence, and to help power companies pre-plan to support critical assets within their service footprints.

<sup>132</sup> Department of Defense, *Department of Defense Directive 3020.40: Mission Assurance (MA)*, November 29, 2016, [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).

<sup>133</sup> Department of Defense, *Department of Defense Manual 3020.45: Defense Critical Infrastructure Program (DCIP): Execution Timeline*, last updated May 23, 2017, <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>

The third circle includes the still larger array of Defense installations, including National Guard bases, which would be essential for providing Defense Support to Civil Authorities (DSCA) if disruptions of the grid jeopardize public health and safety. In Hurricane Maria (2017), superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and providing other assistance. Protecting or rapidly restoring the reliability of the DCEI that supports these DSCA functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public. Ultimately, however, countering such adversary efforts will require protecting grid service to the still broader array of hospitals, water systems, and other civilian assets served by critical electric infrastructure.

## **2. Deterrence by Denial: Protecting Critical Electric Infrastructure**

Emergency orders can also strengthen deterrence through a very different means. In addition to deterring adversaries by threatening to inflict unacceptable costs if they attack, and being able to defeat them abroad if war occurs, the United States can also discourage attacks by making adversaries doubt that those attacks can inflict major disruptions on the grid. The *National Security Strategy* notes that “A stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.”<sup>134</sup> Bolstering such “deterrence by denial” constitutes a prime goal for developing emergency orders, as well as a source of challenging design requirements.

A special advantage of deterrence by denial is that it does not rely on attack attribution to discourage adversaries from striking the grid. Threats to impose unacceptable costs on attackers will only work if adversaries believe that the United States will be able to identify them as the perpetrators. To evade punishment, attackers are likely to take extraordinary technical measures to complicate or defeat such attribution. The Federal Bureau of Investigation and other Federal agencies need to continue strengthening their attribution capabilities accordingly.<sup>135</sup> FPA information sharing mechanisms can support such improvements by helping speed and secure the delivery of malware samples and other threat signature information between utilities and government agencies.<sup>136</sup>

Nevertheless, despite these efforts, sophisticated adversaries may still doubt whether the United States will be able to identify them as the attacker. Emergency orders that bolster grid resilience can support a different means to deter these adversaries. By helping power companies sustain service to essential customers, emergency orders can heighten adversary doubts as to whether

---

<sup>134</sup> President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 13.

<sup>135</sup> Scott S. Smith, “Roles and Responsibilities for Defending the Nation from Cyber Attack,” *Testimony Before the Senate Armed Services Committee*, October 19, 2017. See also: Lily Hay Newman, “Hacker Lexicon: What is the Attribution Problem?,” *WIRED*, December 24, 2016, <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.

<sup>136</sup> See: 16 U.S.C. § 824o–1, Section (d), <https://www.law.cornell.edu/uscode/text/16/824o-1>. Later sections of this study provide a more detailed assessment of provisions for improved information sharing.

attacks will be effective and reduce the expected benefits of striking the grid regardless of U.S. attribution capabilities.

Orders that contribute to deterrence by denial will also be useful against adversaries who do not care that the United States will punish them for attacks on U.S. critical infrastructure. For threats of cost imposition to work, the United States must be able to identify and destroy things that foreign leaders would find intolerable to lose.<sup>137</sup> However, it will be very difficult to target anything that leaders of the Islamic State would find so precious.<sup>138</sup> Deterring cyberattacks through threats of punishment could also be difficult against leaders such as Kim Jong Un.<sup>139</sup> Emergency orders can provide an alternative means to discourage these adversaries from attacking the grid by reinforcing their doubts that they can achieve the disruptive effects they seek.

Finally, emergency orders and the improvements in grid resilience they provide could help U.S. leaders prevail in future confrontations. In regional conflicts that have not yet escalated to full-scale cyberattacks against the United States, U.S. leaders may wish to launch carefully-selected strikes (via cyber or conventional means) against adversaries to encourage them to de-escalate and negotiate for peace. Those leaders may be reluctant to employ strike options if they believe adversaries could cripple the U.S. grid in response. By strengthening the confidence of the President and his advisers that the grid can survive attack(s), and sustain service to essential facilities and functions, emergency orders can help widen the range of options available to the President to resolve future conflicts.<sup>140</sup>

Emergency orders will need to meet stringent design requirements to achieve these goals. To strengthen deterrence by denial, and – if deterrence fails – help ensure that the United States will prevail in a conflict, a large and exceptionally diverse set of customers will need resilient power.

---

<sup>137</sup> Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 3.

<sup>138</sup> Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 4; Brian Michael Jenkins, “Countering al-Qaeda: The Next Phase in the War,” *RAND*, September 8, 2002, <https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html>.

<sup>139</sup> Egle Murauskaite, “North Korea’s Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment,” *38 North (US-Korea Institute at Johns Hopkins SAIS)*, September 12, 2014, <http://www.38north.org/2014/09/emurauskaite091214/>. In contrast, James Andrew Lewis argues that “the primary objective of the North Korean state and the Kim family is regime survival” and they will be loath to put that survival at risk by striking the U.S. grid and other critical infrastructure. James A. Lewis, “North Korea and Cyber Catastrophe—Don’t Hold Your Breath,” *38 North (US-Korea Institute at Johns Hopkins SAIS)*, January 12, 2018, <http://www.38north.org/2018/01/jalewis011218/>. On the broader challenges of tailoring threats of punishment to deter specific nations and foreign leaders, see Defense Science Board, *Task Force on Cyber Deterrence*, February 28, 2017, p. 12.

<sup>140</sup> Even if the United States greatly strengthens grid resilience, the use of cyber weapons in future conflicts will be fraught with risks of rapid (and perhaps unintended) escalation. Jim Miller and Richard Fontaine argue that structural incentives exist for rapid escalation in cyberspace, and that adversaries will have incentives to employ cyber capability “in large doses early in a major conflict to gain coercive and military advantage – and to attempt to prevent the other side from gaining such an advantage.” Miller and Fontaine, *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies are Reshaping Pathways to Crisis and Conflict*, September 2017, p.16.

See also: Jason Healy, “The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities,” *Columbia University*, June 2016, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2836206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206).

Only a limited set of military bases and supporting civilian assets are critical to the defense of the United States. However, adversaries may seek to not only disrupt U.S. Defense capabilities, but also jeopardize societal continuity by crippling electric service to regional hospitals, major financial institutions, and other facilities essential to the U.S. economy and public health and safety.

### **3. Building a “Section 9+ List:” Prioritizing Infrastructure for Sustainment and Restoration**

The Federal Power Act emphasizes the need to protect and restore CEI which, if destroyed or incapacitated, would “negatively affect” national security, the U.S. economy, and public health or safety. But such effects could result from the loss of power to many thousands of hospitals, water utilities, communications systems, and other assets spread across all 16 critical infrastructure sectors. Industry and government do not have the operational resources required to sustain and rapidly restore all critical infrastructure that may be impacted by a large-scale attack.

DOE and its private sector partners will therefore need to pre-identify a far more specific and stringently-prioritized list of critical assets and supporting CEI to protect. To develop template emergency orders and contingency plans to implement them, industry and government will need to determine which specific customers (and the critical electric infrastructure that serves them) are the most critical recipients of prioritized power flows if normal service breaks down.

Executive Order 13636 (February 2013) provides the best methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the Secretary of Homeland Security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.”<sup>141</sup> That standard – catastrophic damage – provides a basis to identify the highest priority assets and associated CEI for protection by emergency orders in GSEs. Over time, orders and contingency plans could gradually encompass less critical facilities and grid infrastructure.

Of course, the Section 9 methodology and subsequent list were never intended to support the implementation of Section 215A of the FPA. As a result, the Section 9 methodology falls short of meeting all the requirements for supporting emergency order design. This methodology, for example, is designed specifically for cybersecurity incidents. Meanwhile, the FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on critical grid assets. EO 13636’s Section 9 requirements also create a “corporate” level list that is not broken down to the key priorities within the corporation (i.e., facilities, systems, and nodes). Identifying the most critical assets and facilities as priorities in GSEs will require a more fine-grained analysis which considers the increasingly complex interdependencies of U.S. critical infrastructure.

---

<sup>141</sup> Executive Order 13636 – *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

Despite these shortfalls, DHS' Executive Order 13636 methodology can provide a valuable starting point for identifying the most vital CEI and supporting assets. DOE and its industry partners should leverage that methodology to create a "Section 9+" list, tailored to fulfill FPA emergency order requirements. Other government efforts to prioritize critical infrastructure, could also make valuable contributions to the list and overall prioritization effort.<sup>142</sup> However, further impediments exist to ensuring that such a list will be effective.

The Section 9 methodology, for example, lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the Federal government tells grid owners and operators if they are on the Section 9 list, they are rarely informed about the Section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data. The Federal government will therefore face inherent problems in building a list of the most critical infrastructure assets and components nationwide.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that individual pharmaceutical distributors, suppliers of water system treatment chemicals, and other companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations in one industry can produce unintended and unforeseen effects on overall system resilience. Yet, companies have powerful incentives to resist sharing such business-sensitive, proprietary information. Public sector leaders will therefore have to strengthen their industry counterparts' confidence that government agencies would not use this data for regulatory compliance, antitrust, or other purposes not explicitly approved through industry-government dialog.

---

<sup>142</sup> There are numerous examples. DHS' National Critical Infrastructure Prioritization Program (NCIPP) aims to identify "nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance." See: DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, p. 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on "lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity." *Ibid.*, at p. 30. Despite its focus on terrorist threats, HSPD-7 also requires the Secretary of Homeland Security to identify and prioritize systems and assets, which, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. DHS, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, <https://www.dhs.gov/homeland-security-presidential-directive-7>. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the "loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States" and lower jurisdictions. The national level priorities on this list could also be helpful. Section (a)(2), 6 U.S.C. § 1241 – *National asset database*, <https://www.law.cornell.edu/uscode/text/6/1241>.



Securing and containing the distribution of this classified data will also be a crucial consideration. The Section 9+ list or equivalent prioritization efforts, if obtained by adversaries, would serve as an instructive guide on how to maximize the devastation of U.S. critical infrastructure and provide a strategic roadmap for attack. To ensure the Section 9+ list's utility in enabling planning and order design, however, essential efforts to protect this data must be complemented by an improved scheme for providing the data to appropriate individuals (with the required security clearance).

## **B. COMMUNICATIONS REQUIREMENTS FOR ISSUING AND EMPLOYING EMERGENCY ORDERS**

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phone and other normal means of communication fail. Under the Electricity Subsector Coordinating Council (ESCC), they have also built an extensive set of “playbooks” to help companies decide what to tell customers about the incident, and to create “unity of messaging” between government officials and industry representatives on estimated times of restoration (ETRs) and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. In anticipation of attacks causing grid security emergencies, these partners have the opportunity to focus on three specific challenges: 1) maintaining survivable communications systems for issuing and sustaining the implementation of emergency orders; 2) preventing adversaries from gaining access to sensitive emergency orders and classified information; and 3) determining what to say to the U.S. public about the attack, potentially including strategies for countering adversary efforts to intensify public panic and incite disorder.

Requirements for survivable and secure communications will be widely shared across many types of grid security emergencies and template EOs. The section that follows offers recommendations to help meet these common needs. In contrast, for informing the U.S. public as to why the Secretary has issued emergency orders and what customers should expect, “no regrets” conservative operations will generate only minor challenges compared to prioritized load shedding and other orders that disrupt normal service. Pre-planning for such “strategic messaging” will be vital to counter the political leverage that adversaries will seek by attacking the grid and should be an integral part of the emergency order design process.

### **1. Communications Requirements in Grid Security Emergencies**

As with the phases of grid security emergency declarations (starting when attacks are imminent), the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Pre-attack

consultations constitute the initial stage. The Federal Power Act specifies that before the Secretary issues EOs, DOE will consult with power companies and other BPS stakeholders “to the extent practicable...regarding implementation of such emergency measures.”<sup>143</sup> This study also recommends that Federal officials consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The Final Rule on *Grid Security Emergency Orders: Procedures for Issuance* clarifies how DOE’s Office of Electricity Delivery and Energy Reliability (OE) will consult on EOs. The GSE Rule specifies that, if practicable, the Electricity Information Sharing and Analysis Center (E-ISAC) is one of the organizations with which the Secretary will consult. Such consultations will be especially useful for sharing data (including classified data) on attacks that are imminent or underway. The GSE Rule also notes that OE will consult with the Electricity Subsector Coordinating Council (ESCC). The ESCC will provide an especially valuable source of industry perspectives on GSE declarations and EOs because the Council represents all components of the electricity subsector and has extensive experience in coordinating industry incident response operations. In addition, the GSE Rule states that “efforts will be made” to consult with NERC, regional entities such as Regional Transmission Operators, “owners, users or operators” of CEI and DCEI, appropriate Federal and state agencies, and other grid reliability stakeholders.<sup>144</sup>

Issuing emergency orders constitutes the second stage. The GSE Rule states that DOE will “communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances.”<sup>145</sup> However, DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.<sup>146</sup> Doing so will be much more efficient and effective than creating a separate, unfamiliar system for communicating emergency orders. Using established communication systems also has the added benefit of pre-existing legitimacy, which can help DOE and utilities avoid potential questions over authentication and possible adversary attempts to spoof EOs. Industry should provide recommendations to DOE on how best to communicate orders to BPS entities to ensure they will be effectively implemented.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders and monitor their compliance with those EOs. Attacks on the grid are unlikely to be “one and done.” As adversaries continue to try to create grid instabilities, and power companies respond with emergency operations to prevent cascading failures, maintain service to critical facilities, and restore power while under attack, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional EOs and response activities – potentially on a nationwide basis. Reliability Coordinators (RCs) will be a critical touchpoint between DOE and individual

---

<sup>143</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1774

<sup>144</sup> *Ibid.*, at p. 1181.

<sup>145</sup> *Ibid.*

<sup>146</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1177

BPS entities. RCs can serve as a focal point between DOE and other government leaders and the BPS entities which are in their purview.

Sustained communications will also be necessary to meet an additional requirement of the Federal Power Act: enforcement of emergency orders. The GSE Rule specifies that “Beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order.”<sup>147</sup> Moreover, “in accordance with available enforcement authorities, the Secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order.”<sup>148</sup>

## **2. Survivability of Communications**

Adversaries will have compelling incentives to combine attacks on the grid with strikes against U.S. communications systems. The 2015 attack on Ukraine’s electric system illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone system; the latter attack prevented customers from reporting outages and disrupted the ability of grid operators to focus on restoration operations accordingly.<sup>149</sup> In turn, if adversaries can lengthen power outages by disrupting communications systems essential for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually-reinforcing disruptions in both sectors.

We should assume that adversaries will attack to maximize these failures, especially since they would already be facing the risk of U.S. response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry-government coordination in grid security emergencies.

The likelihood of such combined attacks will intensify as DOE and its partners move through the sequential communications stages of grid security emergencies. Risks will be lowest in the consultation phase. That is fortunate. Under the ESCC, the electric industry has created extensive mechanisms to coordinate response operations by multiple power companies and coordinate mutual assistance operations with DOE and other government agencies. Consultations on possible emergency orders will leverage that existing ESCC system.

To date, however, ESCC consultations on response operations have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to

---

<sup>147</sup> *Ibid.*, at p. 1182.

<sup>148</sup> *Ibid.*

<sup>149</sup> “Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure,” *ICS-CERT*, February 25, 2016, <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.

distributed denial of service (DDoS) attacks and a range of other increasingly severe threats,<sup>150</sup> as well as the communication sector's reliance on grid-provided electricity (especially in long duration outages that put emergency power assets at risk).

The GSE Rule notes the Department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include "essential actions" to protect bulk power system reliability which require recipients to respond as defined in the alert.<sup>151</sup> DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across the bulk power system. NERC already distributes alerts broadly to users, owners, and operators of the bulk power system in North America. Hence, for issuing emergency orders, the alert system provides DOE with an opportunity for "one stop shopping." The Secretary could issue an order to NERC for distribution to both regional operating organizations (RTOs, ISOs, Reliability Coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is e-mail-based.<sup>152</sup> As a result, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also only includes those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for sustaining power to critical facilities and for implementing emergency orders for prioritized load shedding and other actions.

Industry and government partners should consider additional measures to bolster that alert system or create fallback options for the Secretary to issue orders when attacks are underway. Satellite phones may provide an especially prominent option. Those phones are widely deployed both by BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies. General William Shelton (USAF-Ret.) who directed the U.S. Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these

---

<sup>150</sup> Russ Banham, "DDoS Attacks Evolve To Conscript Devices Onto The IoT," *Forbes*, February 4, 2018, <https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#4b5a43a86aaa>.

<sup>151</sup> "About Alerts," *NERC*, n.d.a., <http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx>.

<sup>152</sup> *Ibid.*

counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community.”<sup>153</sup>

The most difficult challenges for communications in a GSE would emerge as BPS entities implement emergency orders, and power companies coordinate with DOE on emergency operations and respond to follow-on strikes. Communications systems are likely to be under comprehensive attack during this stage. To prepare against that risk, power companies are ramping up their investments in emergency communications systems that are hardened against cyber and physical attacks, and can be used to sustain critical grid functions even if satellite phones fail.<sup>154</sup> Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are underway in building dark fiber or other survivable links between BPS entities – much less between those entities and DOE. The National Infrastructure Advisory Council study on *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish “separate, secure communications networks specifically designated for the most critical cyber networks, including ‘dark fiber’ networks for critical control system traffic and reserved spectrum for backup communications during emergencies.”<sup>155</sup>

The study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities “can communicate with utility crews working in the field to manually restore power” and conduct other post-attack operations.<sup>156</sup> Survivable communications systems will also need to enable the same multi-company decision-making and coordination with government that the ESCC already employs for hurricanes and other natural disasters. The development and deployment of such systems must be part of broader effort to prepare for grid security emergencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when they are needed most.

### **3. Securing Sensitive Emergency Orders and Classified Information**

Certain types of emergency orders may be vulnerable to countermeasures if adversaries gain access to them. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as

---

<sup>153</sup> General William L. Shelton, USAF (Ret), “Threats to Space Assets and Implications for Homeland Security,” *Written Testimony Before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*, March 29, 2017, p. 3, <http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf>.

<sup>154</sup> Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC), *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans – Further Joint Study: Planning Restoration Absent SCADA or EMS (PRASE)*, June 2017, p. 15.

<sup>155</sup> NIAC, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, August 2017, p. 7. <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>

<sup>156</sup> *Ibid.*



possible, lest those operations create incentives for adversaries to strike before their APTs were disabled. When attacks are underway, it could be useful to deny adversaries the knowledge of where and how BPS entities were prioritizing the flow of power to key military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The Federal Power Act and subsequent GSE Rule provide for the sharing of classified information in grid security emergencies. The GSE Rule specifies that:

To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.<sup>157</sup>

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program (CRISP) already have mechanisms and protocols for sharing and securing classified threat data with BPS entities cleared for access to that data.<sup>158</sup> Industry and government partners should consider building on those mechanisms to support the issuance of classified EOs. However, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Moreover, for utilities with cleared personnel on their staffs, an even smaller number possess the Sensitive Compartmented Information Facilities (SCIFs) or other infrastructure and government approvals to store classified information. To address those limitations, the GSE Rule clarifies that the Secretary may declassify information critical to the emergency response.<sup>159</sup> But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of Combatant Commander operational plans; when EOs may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

#### **4. Communicating with the American People**

Adversaries may attack the grid not only to disrupt national defense and the economy, but also to gain political leverage over U.S. leaders by inciting public panic and disorder. A presidential declaration that the grid faced imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks

---

<sup>157</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1182.

<sup>158</sup> “Energy Sector Cybersecurity Preparedness,” *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

<sup>159</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1778.

and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the U.S. public.

Pre-planning for public messaging to accompany GSE declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Providing for unity of messaging with governors and other elected officials on estimated times of restoration (ETRs) can present significant challenges in such events. However, those difficulties will be dwarfed by the problems that cyberattacks will create. GridEx IV (November 2017) highlighted a number of such problems. They include:

- Adversary use of information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety;
- Disruption of normal means of communication on which the public will rely for information about the event; and
- Inherent difficulties of estimating ETRs when adversaries employ advanced persistent threats that enable repeated re-attacks and disruptions in grid service until eradicated from BPS networks.

The ESCC and its members are developing playbooks to help meet these challenges, and to support public messaging in the event of cyber or physical attacks against the grid.<sup>160</sup> Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that Presidential GSE declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Pre-planning for message coordination with Canada and Mexico could also be helpful and might leverage the Federal Power Act's provisions for such multi-national consultations concerning the issuance of emergency orders.<sup>161</sup>

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. Some orders that will be valuable for protecting grid reliability, including EOs for prioritized load shedding, could cut off electricity to many thousands of customers in order to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by pre-planned communications playbooks to address customer concerns.

### **C. THE DEEPER VALUE PROPOSITION FOR EMERGENCY ORDERS: ENFORCEMENT, WAIVERS, AND COST RECOVERY**

---

<sup>160</sup> "ESCC," *Electricity Subsector Coordinating Council*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.

<sup>161</sup> 16 U.S.C. § 824o-1, Section (b)(3), <https://www.law.cornell.edu/uscode/text/16/824o%E2%80%931>.

Conservative operations offer an attractive starting point to develop pre-attack emergency orders because so many power companies already have extensive, frequently-used COs in place. For post-attack orders, NERC reliability standards provide a similarly well-established foundation for load shedding and other extraordinary measures. Emergency orders to accelerate power restoration can draw on a mutual assistance system that utilities have been refining for decades. These existing means of protecting and restoring grid reliability are so effective that they beg the question: how can emergency orders add value for defending the bulk power system and provide benefits beyond those that industry-based measures already offer?

EOs provide a unique means to ensure that BPS entities' emergency plans directly support U.S. deterrence goals and other national security priorities. As DOE and its partners identify critical electric infrastructure and defense critical electric infrastructure, and share that data with BPS entities, the electric industry will also be better positioned to develop utility-specific plans to sustain or restore service to vital facilities.

The development of template emergency orders will provide other benefits as well. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting COs to meet the specialized challenges posed by cyber and physical threats.<sup>162</sup> The industry-government process to develop emergency orders will provide a basis to share emerging best practices and embed them in utility plans for grid security emergencies.

The EO development process will also help protect grid reliability against nationwide threats. While hurricanes and other familiar natural hazards affect only limited geographic areas, adversaries may use cyber weapons to simultaneously attack all three interconnections in the United States. Communicating EOs in real time to utilities across the country may pose a challenge. DOE and the electricity subsector already have mechanisms in place to alert utilities when adversaries are implanting malware on critical systems, including the Cybersecurity Risk Information Sharing Program (CRISP) and other E-ISAC notification procedures and portals.<sup>163</sup> This includes the E-ISAC's new "Critical Broadcast Program," which is intended to operationalize their information sharing capabilities.<sup>164</sup> The Federal Bureau of Investigation (FBI) and DHS also issue alerts to the energy sector, as in the case of Nuclear 17 (June 2017)

---

<sup>162</sup> See, for example, PJM, *PJM Manual 13: Emergency Operations* Revision 64, June 1, 2017, p. 73; Todd Lucas (Southern Company), "Conservative Operations," (presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, Colorado, September 18-19, 2013), <http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf>; and SERC Reliability Corporation, *Conservative Operations Guidelines* Guide-800-101, May 20, 2015, [https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines\\_rev-0-\(05-20-15\).pdf?sfvrsn=2](https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2).

<sup>163</sup> "Energy Sector Cybersecurity Preparedness," *Department of Energy*, n.d.a., <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>; "Electricity ISAC," *NERC*, n.d.a., <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.

<sup>164</sup> The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See: Bill Lawrence, Charlotte de Seibert, and Philip Daigle, "E-ISAC Update," (presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, Florida, March 6-7, 2018), <https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf>.

and Crash Override.<sup>165</sup> However, when the President determines that there is an imminent danger of attacks on the grid, the Secretary will need a speedy and reliable system to trigger the implementation of conservative operations (including, potentially, specialized malware search and eradication measures) on a nationwide basis. Leveraging existing alert systems to support the issuance and execution of EOs will expedite preparedness for GSEs. It will also be essential to assess how adversaries might seek to disrupt the use of these existing systems, and supplement them as needed.

Developing EOs will facilitate nationwide exercises as well. NERC already requires BPS entities to exercise their individual emergency plans. In the GridEx exercise series, over 100 utilities across the United States and Canada exercise their plans against combined cyber-physical attacks and have an opportunity to share lessons learned. Building template emergency orders and utility-specific implementation plans would provide an even stronger basis for coordinated, multi-entity exercises against a notional threat, including the issuance and execution of emergency orders for all three phases of grid security emergencies.

Beyond these preparedness benefits, specific components of the Federal Power Act and GSE Rule create additional opportunities for added value – particularly if industry and government partners plan in advance for their mutual benefit.

## **1. Enforcement and Political “Top Cover”**

The GSE Rule specifies that “in accordance with available enforcement authorities, the Secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that order.”<sup>166</sup> The prospect that BPS entities will be punished for refusing to comply with poorly-conceived orders could raise concerns over the possible misuse of the Secretary’s enforcement powers. To help address those concerns, the Rule lays out a process by which entities can request clarification or reconsideration of orders issued to them.<sup>167</sup> How that process would actually function in the midst of nationwide attacks on the grid is uncertain.

However, pre-event coordination between industry and government could turn the looming threat of mandatory EO compliance into a mutually-beneficial arrangement. Rather than rely solely on adjudication mechanisms after the Secretary issues orders, DOE should collaborate with utilities to develop and refine orders in ways consistent with existing utility emergency procedures and

---

<sup>165</sup> The initial July alert was sent directly to energy sector stakeholders. See: Ellen Nakashima, “U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks,” *Washington Post*, July 8, 2017, [https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47\\_story.html?utm\\_term=.6ba8bdc7d36f](https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?utm_term=.6ba8bdc7d36f). FBI and DHS later released a public alert in October 2017. See: “Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors,” *United States Computer Emergency Readiness Team*, October 20, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-293A>. For the CrashOverride alert, see: “Alert (TA17-163A) CrashOverride Malware,” *United States Computer Emergency Readiness Team*, June 12, 2017, <https://www.us-cert.gov/ncas/alerts/TA17-163A>.

<sup>166</sup> Department of Energy, “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40),” *Federal Register* Vol. 83, No. 7 (2018), p. 1182.

<sup>167</sup> *Ibid.*, at pp. 1181-1182.

operational constraints. Doing so would – ideally – transform the mandatory nature of EOs into an advantage for utilities rather than a potential problem by leveraging the benefits that EOs provide for actions that these utilities would ordinarily carry out to protect or restore their systems. As examined in the two following sub-sections, those benefits include indemnification from environmental and other regulatory requirements, and the potential to recover costs incurred while carrying out the orders. With proper consultation, mandatory EOs could therefore serve to protect and compensate utilities for the very emergency actions required to protect their own systems.

The mandatory nature of EOs would also strengthen industry-wide security measures. NERC-developed (and FERC-approved) mandatory reliability standards and requirements to protect critical infrastructure from cyber and physical threats already help protect grid reliability against attacks by providing for consistent, nationwide adherence to those standards and the planning, training, and exercising requirements they entail. Some utilities voluntarily take further measures necessary to protect their systems from cyber threats. However, due to the interconnected nature of the BPS, the grid is only as strong as its weakest links.<sup>168</sup> The disparity in BPS entities' hardening efforts against adversarial threats means that even those that exceed NERC standard requirements remain potentially vulnerable. Creating mandatory emergency orders could help bridge the gap in protection against grid security emergencies, especially if BPS entities help shape those orders to go above and beyond the benefits of existing mandatory provisions for reliability.

Response operations provide an immediate opportunity to achieve such “value added” in designing EOs. The Electricity Subsector Coordinating Council serves as the principal liaison between the Federal government and the electric industry in responding to severe power outages. The Council includes entities of all ownership structures in the subsector, including investor-owned utilities, electric cooperatives, municipally-owned utilities, and federal utilities. This industry-wide representation enables the ESCC to serve as the “center of gravity” for coordinating response operations with DOE and other government partners. Moreover, after decades of use in hurricanes and other severe natural hazards, the Council's collaborative mechanisms offer a strong, industry-developed and time-tested basis for responding to grid security emergencies.

The ESCC is already adapting its response coordination mechanisms to support restoration against manmade threats – most notably by establishing a Cyber Mutual Assistance program.<sup>169</sup> Moreover, following Superstorm Sandy, investor-owned utilities (led by the Edison Electric Institute) also established new mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States under the National Response Event

---

<sup>168</sup> Department of Energy, *Quadrennial Energy Review – Transforming the Nation's Electricity System: Second Installment of the QER*, January 2017, p. 1-33.

<sup>169</sup> Electricity Subsector Coordinating Council, *The ESCC's Cyber Mutual Assistance Program*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.2>.



(NRE) framework.<sup>170</sup> Both initiatives will be vital for responding to grid security emergencies that entail multi-region disruptions of the BPS.

The representative structure of the ESCC provides additional advantages for preparedness against GSEs. While only a limited number of industry CEOs service on the Council at any one time, those CEOs are able to reach out to other grid owners and operators across the United States and help coordinate the provision of restoration personnel and equipment on a nationwide basis. These CEOs can also request additional resources and strategic guidance when available response assets are stretched thin. However, all such assistance is voluntary; the ESCC lacks the authority to require utilities to provide assistance or to prioritize restoration operations when available resources cannot meet all requests for aid.

Emergency orders could offer DOE an additional means to support industry response operations and ensure that they account for government priorities. The Department's support could be especially valuable against cyberattacks. When hurricanes strike the Gulf Coast or the Southeast, for example, utilities on the West Coast can contribute response crews, bucket trucks, and other response assets, safe in the knowledge that the storm will not affect their own service areas. Cyberattacks will create a very different environment for providing voluntary assistance. Attacks on one utility may presage an attack on all. Utility CEOs who donate scarce cyber response personnel and assets to support another company will be at risk of suffering similar attacks, and – potentially – of suffering more severe blackouts because those personnel were already committed elsewhere.<sup>171</sup> The Cyber Mutual Assistance (CMA) Program is developing specialized protocols to deal with these challenges. However, as the ESCC notes, “participation in the CMA Program, as well as any decision to respond to requests for assistance made under the CMA Program, is voluntary.”<sup>172</sup> While the emergency order process will need to take into account the risk of re-attack in cyber incidents, EOs could nevertheless mandate compliance with industry-government decisions on restoration priorities, and reinforce the subsector's voluntary system for providing assistance in National Level Events.

Utilities may also find it helpful that their actions to meet broader national priorities, which are likely to provoke intense opposition from state and local government leaders, state Public Utility Commissioners, and customers, will be Federally-mandated. In Superstorm Sandy and other severe weather events, governors have sometimes been reluctant to support the flow of power restoration crews and equipment to neighboring states until all of their own citizens (read: voters) had their lights back on. Cyber and physical attacks on the grid could create still stronger political disincentives to share restoration assets, especially if adversaries use information warfare to inflame citizen fears over potential outages and threats to public safety. Such attacks could also put utility CEOs in the unenviable position of having to manage shortfalls in available

---

<sup>170</sup> Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, October 2016,

[http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA\\_101FINAL.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf).

<sup>171</sup> North American Electric Reliability Corporation, *Cyber Attack Task Force: Final Report*, March 2012, p. 29, [http://www.nerc.com/%20docs/cip/catf/12-CATF\\_Final\\_Report\\_BOT\\_clean\\_Mar\\_26\\_2012-Board%20Accepted%200521.pdf](http://www.nerc.com/%20docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf).

<sup>172</sup> Electricity Subsector Coordinating Council, *The ESCC's Cyber Mutual Assistance Program*, January 2018, <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.2>.

power by depriving lower priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The Secretary of Energy can give CEOs political top cover for taking such unpopular actions, rather than leave utility leaders to act on a voluntary basis and bear the full brunt of explaining why they did so – or have them not serve national priorities at all.

## **2. Environmental, Regulatory, and Legal Waivers**

In amending the Federal Power Act to address grid security emergencies, Congress also provided power companies with an important protection for complying with emergency orders – one which they might not receive by implementing conservative operations or other emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate grid reliability standards approved by the Federal Energy Regulatory Commission (FERC) or other rules or provisions under FPA, the Act specifies that those actions “shall not be considered a violation” of those provisions. Such waivers of enforcement apply unless a complying entity acts in a “grossly negligent manner.”<sup>173</sup>

The FAST Act amendments to the FPA also introduced broader protections into section 202(c) which absolve entities from violations of Federal, state or local environment law or regulation that occur as a result of complying with an order. That provision also shields complying entities from “any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation.”<sup>174</sup> These protections also apply to Section 215A emergency orders.<sup>175</sup>

These waivers will be especially valuable for certain types of emergency orders. For example, if the Secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service could also violate FERC-approved reliability standards. Separating pre-planned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards.

The waiver process under the FPA is structured to function smoothly and automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that, in the course of complying with an emergency order, a BPS entity has acted in “a grossly negligent manner.” Nevertheless, specifying the waiver protections provided by a given EO, specific to what the Secretary is ordering entities to do, could benefit the collective response to grid security emergencies. In particular, identifying the protections provided by the EO would give complying entities assurances of their protection, and limit potential disputes with regulatory bodies.

Moreover, for certain types of emergency orders, pre-planning for regulatory waivers could comprise a necessary component of the order development process. For example, the amended

---

<sup>173</sup> 16 U.S.C. § 824o–1, Section (f)(4), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

<sup>174</sup> 16 U.S.C. § 824a, Section (c)(3), <https://www.law.cornell.edu/uscode/text/16/824o>.

<sup>175</sup> 16 U.S.C. § 824o–1, Section (f)(2), <https://www.law.cornell.edu/uscode/text/16/824o-1>.

FPA does not provide waivers for Nuclear Regulatory Commission (NRC) regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the NRC would enforce a violation of their regulations by a nuclear generation entity complying with an EO. The worst time to adjudicate such a dispute, however, would be in the midst of a GSE. DOE should therefore engage with the NRC to examine waiver options (or, potentially, options to exclude nuclear generators from EO requirements) as the EO development process goes forward.

Pre-planning will also be vital for EOs that accelerate power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that “the storage of strategically located spare large power transformers” and other critical grid components “will reduce the vulnerability of the United States to multiple risks facing electric grid reliability,” including cyber and physical attacks.<sup>176</sup> Accordingly, Congress required DOE to develop a Strategic Transformer Reserve Plan to determine the number and type of spare Large Power Transformers (LPTs) that should be stored, and examine issues associated with transporting those spares.<sup>177</sup>

DOE responded by providing a Strategic Transformer Reserve (March 2017) report. The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a larger pool of spare LPTs than DOE had anticipated and that a Federally-owned reserve is not needed.<sup>178</sup> However, the Plan also found that it was also crucial to ensure that LPTs can be efficiently moved during national emergencies.<sup>179</sup>

Emergency orders can play a critical role in facilitating that movement. The higher voltage classes of LPTs, including 765 kilovolt (KV) transformers, are as big as a house and can only be moved – slowly and very carefully – by specialized heavy-haul trucks, rail cars, and barges. Under the auspices of the ESCC, utilities have established a Transformer Transportation Working Group to analyze the problems posed by the emergency movement of LPTs and build collaborative plans with transportation companies and associations. A key finding of the Group’s analysis: regulatory waivers will be critical to expedite LPT movement, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.<sup>180</sup>

---

<sup>176</sup> “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1779, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>177</sup> *Ibid.*, at pp. 1780-1782.

<sup>178</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 21, <https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>179</sup> “Fixing America’s Surface Transportation Act,” Public Law 114-94, *U.S. Statutes at Large* 129 (2015): p. 1781, <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.

<sup>180</sup> ICF (for the Department of Energy), *Assessment of Large Power Transformer Risk Mitigation Strategies*, October 2016, pp. 22-23, <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf>.

DOE's 2017 transformer report committed the Department to coordinating with the Transformer Transportation Working Group (TTWG) "to improve and optimize transportation planning in response to a significant national event impacting the electricity grid."<sup>181</sup> However, the report did not examine how emergency orders and implementation plans might speed LPT transportation. As DOE collaborates with the TTWG and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols not addressed by the FPA that pose the greatest impediments to LPT movement, and pre-plan to waive them if the President declares a GSE.

Those coordination efforts will face an immediate challenge: the Secretary of Energy lacks the statutory authority to waive key transportation regulations. Most Federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of the U.S. Department of Transportation (DOT). Federal regulations and emergency operations that would govern barge movement of transformers, which could be critical for restoring power for coastal cities and along the Mississippi-Ohio river system of inland waterways, are overseen by the U.S. Coast Guard (USCG) and the U.S. Army Corps of Engineers (USACE). State and local transportation regulations and permitting requirements will also pose major impediments to emergency LPT road movement unless adequate waivers are in place to lift them.

The EO development process should therefore include coordination with non-DOE regulatory authorities. The Department of Energy has extensive experience in collaborating with other Federal, state, local, tribal and territorial (SLTT) agencies. That experience has been especially valuable for building plans and improving coordination for restoration operations under the auspices of Emergency Response Function #12 – Energy. Moreover, as individual utilities have created contingency plans for emergency transportation with road, rail, and barge companies, they have also built relationships with SLTT agencies and government leaders. Utilities and DOE should build on those relationships and plans to launch a systematic, integrated effort to provide for regulatory waivers where (under the FPA) enforcement of violations would not automatically be waived.

Over the longer term, industry and government partners should also consider whether complying entities should have protections beyond those currently in the Federal Power Act. Prioritized load shedding for extended periods will create "winners and losers" in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other Section 9+ assets may leave dialysis centers, small urgent care centers, and facilities for special needs citizens with shortfalls in electric service. Cutting off power to lower priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.<sup>182</sup>

---

<sup>181</sup> Department of Energy, *Strategic Transformer Reserve: Report to Congress*, March 2017, p. 22, <https://www.energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.

<sup>182</sup> Alison Frankel, "Can customers sue power companies for outages? Yes, but it's hard to win," *Reuters*, November 9, 2012, <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>.

If these risks of exposure are sufficiently severe, Congress should consider providing additional protections for BPS entities that are complying with emergency orders.

### **3. Cost Recovery for Emergency Operations and Supporting Investments in Grid Infrastructure**

Complying with emergency orders may force utilities to incur costs above and beyond their normal operating expenses. The Federal Power Act states that if FERC determines “that owners, operators, or users of critical electric infrastructure have incurred substantial costs” in complying with an EO, FERC shall “establish a mechanism that permits such owners, operators, or users to recover such costs.”<sup>183</sup> Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other EOs could require reimbursement through FERC-directed mechanisms as well.

The Act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that EOs require owners or operators of DCEI to take emergency measures, the owners or operators of critical defense facilities that rely on such infrastructure “shall bear the full incremental costs of those measures.”<sup>184</sup> Fair warning to the Department of Defense: DOD should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- Attacks create major blackouts and deprive utilities of revenue;
- Emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- Adversaries disrupt financial markets, either through direct cyberattacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.<sup>185</sup>

Power companies are rapidly strengthening their plans and capabilities for cross-sector support with the financial services sector (and with the communications sector on which they depend).<sup>186</sup> These efforts should include the development of contingency plans for financial services

---

<sup>183</sup> The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs “prudently,” and that those costs “cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users. 16 U.S.C. § 824o–1, Section (b)(6)(A), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

<sup>184</sup> 16 U.S.C. § 824o–1, Section (b)(6)(B), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

<sup>185</sup> North American Electric Reliability Corporation, *Grid Security Exercise: GridEx III Report*, March 2016, p. 15, <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.

<sup>186</sup> See, for example, the Strategic Infrastructure Coordinating Council (SICC). Electricity Subsector Coordinating Council, *ESCC Initiatives*, January 2018, <http://www.electricitysubsector.org/ESCCInitiatives.pdf>.



companies (in coordination with the Department of Treasury and DOE) to help utilities meet the time-urgent expenses of responding to grid security emergencies.

In addition, to facilitate the EO reimbursement process provided for in the Federal Power Act, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with EOs will be more difficult once attacks are underway. That is especially true since the text of the FPA leaves substantial ambiguities to resolve – starting with the definition of who are “users” of critical electric infrastructure and therefore potentially eligible for reimbursement.

Such users might well include electricity distribution companies who are not BPS entities (and are therefore not subject to emergency orders), but who could be vital to protect and restore the flow of power between high voltage transmission systems and regional hospitals and other critical facilities. For example, intentional load shedding operations to stabilize the grid are nearly all performed at the distribution level, and distribution providers would also be performing the switching for required to implement rotating blackouts. For the many BPS entities that are not vertically integrated and do not own and operate “local” distribution utilities excluded from the FPA’s BPS definition, it will be essential to include those local distribution providers in contingency plans to execute emergency orders. Given the costs that distribution systems may incur in implementing EOs, FERC and its partners should clarify eligibility for reimbursement and the process by which grid operators will recover their costs as soon as possible.

Cost recovery for investments in grid infrastructure to facilitate emergency orders will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. However, other EOs may be impossible to execute unless BPS entities make additional investments in infrastructure. For vital but remote military bases that are served by a single transmission line, it will be near-useless to order transmission operators to protect or rapidly restore service to those bases if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure they can help defeat U.S. adversaries when the Nation is under attack. DOD will need to ensure it has a cost recovery mechanism to reimburse DCEI owners for making such investments.

For pre-planned power islands to be even remotely viable as an EO design option, many such islands will also require at least some infrastructure construction. Ideally, these pre-planned islands will make use of existing generation, transmission, and distribution assets within their service footprints so that they can separate from the grid and still be able to provide reliable electric service to the Section 9+ assets insider their borders. But many areas that might be designed to function as islands in a GSE will lack adequate infrastructure to do so. The interconnected design of the grid enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Pre-planned power islands will not only lose those reliability benefits, but also have to make do with infrastructure that

utilities built and aligned to be supporting components of the interconnected grid – *not* self-sustaining islands that would be stood up in grid security emergencies. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: many EOs could require spending on new transmission lines and other grid infrastructure in order to be effectively implemented.

The provisions of the FPA pertaining to emergency orders do not explicitly authorize reimbursement for such infrastructure investments. While the Act requires FERC to establish a mechanism to enable owners, users, and operators of CEI and DCEI to recover their costs of complying with emergency orders, those funding provisions do not mention pre-attack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover their costs for infrastructure investments against cyber and physical attacks.<sup>187</sup> FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate EO execution.

Similar discussions will be valuable with state public utility commissions (PUCs). As noted above, distribution systems will likely need to play a vital role in implementing emergency orders. PUCs have primary regulatory authority over distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. Public utility commissions could also make important contributions to reviewing proposed EO implementation plans that would be executed within their respective states, particularly for orders that distribution systems would need to help implement.

The Federal Power Act opens the door to discussions with PUCs over investments and planning to support EO execution. The Act states that FERC and the Secretary of Energy “shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions.”<sup>188</sup> Initiating such discussions with the National Association of Regulated Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has conducted detailed analysis of criteria for assessing the prudence of investments against cyber and physical attacks, and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

---

<sup>187</sup> See, for example: Federal Energy Regulatory Commission (FERC), *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies*, Statement of Policy (96 FERC ¶ 61,299), September 14, 2011; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), April 19, 2004, pp. 10-11 (2004); FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), September 22, 2016, p. 60.

<sup>188</sup> 16 U.S.C. § 824o–1, Section (d)(4), [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).

## **V. CONCLUSIONS AND RECOMMENDATIONS FOR FOLLOW-ON ANALYSIS**

[To be completed by April 30, 2018]

[illegible]

- Enhancing Grid Security Through Public-Private Partnerships Act (H.R. 5240)
  - <https://www.congress.gov/bill/115th-congress/house-bill/5240>
- Energy Emergency Leadership Act (H.R. 5174)
  - <https://www.congress.gov/bill/115th-congress/house-bill/5174>

Energy and Natural Resources Act of 2017 (S. 1460)

- <https://www.congress.gov/bill/115th-congress/senate-bill/1460>
- Leading Infrastructure for Tomorrow's America Act (H.R. 2479)
  - <https://www.congress.gov/bill/115th-congress/house-bill/2479>
- Advancing Grid Storage Act of 2017 (S. 1851)
  - <https://www.congress.gov/bill/115th-congress/senate-bill/1851>
- Grid Cybersecurity Research and Development Act (H.R. 4120)
  - <https://www.congress.gov/bill/115th-congress/house-bill/4120>
- Flexible Grid Infrastructure Act of 2017 (S. 1875)
  - <https://www.congress.gov/bill/115th-congress/senate-bill/1875>
- House Resolution 334
  - <https://www.congress.gov/bill/115th-congress/house-resolution/334>

Let me know if you require anything additional.

Enjoy the rest of your day,

(b) (6)

IT Specialist (INFOSEC)

Federal Energy Regulatory Commission

Office of Energy Infrastructure Security

888 First Street NE, Washington, DC 20426

(b) (6)

--

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed and should not be copied or forwarded to others without the permission of the sender. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and not necessarily those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.





# NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?

**Paul W. Parfomak**

Specialist in Energy and Infrastructure Policy

March 19, 2018

**Congressional Research Service**

7-5700

[www.crs.gov](http://www.crs.gov)

R45135

## Summary

A 2013 rifle attack on a critical electric power substation in Metcalf, CA, marked a turning point for the U.S. electric power sector. The attack prompted utilities across the country to reevaluate and restructure their physical security programs. It also set in motion proceedings in Congress and at the Federal Energy Regulatory Commission (FERC) which resulted in a new mandatory *Physical Security Reliability Standard* (CIP-014) for bulk power asset owners promulgated by the North American Electric Reliability Corporation (NERC) in 2015. In the three years since FERC approved this new standard, security risks to the power grid have become an even greater concern in the electric utility industry. Reflecting these ongoing security concerns, legislative proposals in the 115<sup>th</sup> Congress include provisions directed at power grid physical security. Congress also continues its oversight of grid security and implementation of NERC's security standards.

Three entities play key roles in standards oversight and support of implementation for bulk power physical security. NERC and FERC oversee implementation of the CIP-014 standards, while the Department of Energy plays a supporting role in helping bulk power asset owners to protect their critical infrastructure. The detailed findings of NERC's compliance activities are not publicly disclosed due to their confidential nature. However, NERC has stated that the utility industry is making progress towards effective implementation of the CIP-014 standard and NERC has been "encouraged" by grid security measures put in place so far. NERC compliance audits as of February 2018 have uncovered no major failures to date.

In addition to compliance with NERC's standards, there have been other observable changes within the electricity sector reflecting greater emphasis on bulk power physical security. These changes include realignment in corporate structure to support physical security, incorporating physical security in transmission planning, new security products and services, utility capital investment in physical security, and utility participation in voluntary security programs. While public information about such changes is limited, it suggests they may be significant and widespread.

Although the electric power sector seems to be moving in the overall direction of greater physical security for critical assets, many measures have yet to be implemented and the process of corporate realignment around physical security is still underway. NERC's CIP-014 standards have been promulgated recently, and bulk power asset owners have largely begun enhancing physical security under the standard over the last two years. Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector's own assessments of risk. Bulk power security remains a work in progress.

Congress continues to be concerned about the current state of electric grid physical security. Among many specific issues of potential interest, Congress may focus on several with policy significance: security implementation oversight, cost recovery, hardening vs. resilience, and the quality of threat information. As CIP-014 implementation and other physical security initiatives proceed, Congress also may seek to maintain its focus on the power sector's overall progress, not only on short term compliance with NERC's security standards, but also on structural changes supporting physical security as a priority far into the future.

## Contents

Introduction .....	1
Power Grid Threat Environment .....	2
NERC's Physical Security Standards .....	3
Physical Security Standard Requirements.....	4
Federal Oversight and Support.....	4
NERC's Implementation Oversight .....	5
Electricity Information Sharing and Analysis Center .....	6
FERC Oversight.....	7
DOE Initiatives.....	8
Observed Changes in Bulk Power Physical Security .....	9
Corporate Structure Supporting Physical Security.....	9
Physical Security in Long-Term Transmission Planning .....	11
New Security Products and Services.....	12
Capital Investment in Physical Security.....	13
Utility Participation in Voluntary Security Programs.....	14
NERC Grid Security Exercises.....	14
DHS Critical Infrastructure Surveys .....	15
Legislative Proposals in the 115 <sup>th</sup> Congress .....	15
Policy Issues for Congress.....	16
Oversight of Physical Security Implementation.....	17
Financial Requirements and Cost Recovery .....	18
Hardening vs. Resilience.....	18
Threat Information .....	19
Conclusion.....	20

## Contacts

Author Contact Information .....	21
----------------------------------	----

## Introduction

Securing the electric power grid is among the highest priorities for critical infrastructure protection in the United States. In the past, power grid facilities have had varying degrees of access control and surveillance depending upon the facility type and location. These measures were largely focused on public safety (reflecting liability concerns) and preventing vandalism and theft. More recently, federal agencies, Congress, and the utility industry have focused greater attention on the vulnerability of the power grid, especially the high voltage transmission (bulk power) system, to terrorist attacks which could cause widespread, extended blackouts.

Until 2013, the emphasis of analysts and policymakers was on power grid cybersecurity—protecting the computer controls and communication systems used to operate the grid. However, a 2013 rifle attack on an electric transmission substation in Metcalf, CA, shifted more attention to the physical security of power grid critical assets. In response to the Metcalf attack, as well as other grid incidents and findings from utility security exercises, Congress passed new legislation to strengthen power grid physical security and to facilitate recovery in the event of a successful attack.<sup>1</sup> Congress also sought stronger physical security standards from the Federal Energy Regulatory Commission (FERC) under the commission’s existing statutory authority to regulate the reliability of the bulk power system. FERC, in turn, ordered the North American Electric Reliability Corporation (NERC)—the not-for-profit organization responsible for ensuring grid reliability—to promulgate new requirements for the physical security of bulk power critical infrastructure.<sup>2</sup> After consultation within the utility industry, NERC proposed new physical security standards in May 2014. FERC approved them, with minor changes, the following November.<sup>3</sup>

Since 2014, security risks to the power grid have become an even greater concern in the electric utility industry. Addressing them has remained a concern of Congress.<sup>4</sup> An emphasis on physical risk to the power grid was underscored in September 2016 by another successful rifle attack on a transformer substation—in Utah. Reflecting ongoing security concerns, legislative proposals in the 115<sup>th</sup> Congress include provisions directed at power grid physical security. Congress also continues its oversight of FERC’s grid security activities and the implementation of NERC’s physical security standards.

This report examines changes to the physical security of the electric power grid since the promulgation of NERC’s physical security standards. The report discusses the current risk environment for the bulk power system. It summarizes the key requirements of NERC’s security standards, including its applicability to specific assets, implementation deadlines, and oversight. The report reviews observable changes in the utility sector related to physical security. It concludes with an overview of proposed legislation and a discussion of policy issues for Congress.

---

<sup>1</sup> The Fixing America’s Surface Transportation (FAST) Act (P.L. 114-94), which became law on December 4, 2015, contains provisions to protect or restore the reliability of critical electric infrastructure or defense of critical electric infrastructure during a grid security emergency (§1104).

<sup>2</sup> Among other functions, NERC develops and enforces reliability standards, monitors the grid, and trains industry personnel. In the United States, NERC is subject to Federal Energy Regulatory Commission oversight.

<sup>3</sup> For more historical background and details regarding the development of NERC’s standards, see CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak.

<sup>4</sup> See for example: Senator Ron Johnson, Chairman, Opening statement before the Senate Committee on Homeland Security and Governmental Affairs hearing on “Threats to the Homeland,” September 27, 2017.

This report focuses primarily on physical security efforts to prevent successful physical attacks on the bulk power system. For analysis of issues specifically related to power grid cyberattacks and cybersecurity, see CRS Report R43989, *Cybersecurity Issues for the Bulk Power System*, by Richard J. Campbell. This report also does not address issues related to security incident recovery or restoration, except in the context of preventive physical security.

## Power Grid Threat Environment

Grid security analysts and policymakers have long been aware of physical risks to bulk power critical infrastructure, especially to high voltage (HV) transformer stations and substations, which serve as key nodes within the electric transmission system.<sup>5</sup> The 2013 Metcalf attack, in which an unknown perpetrator firing a .30 caliber rifle disabled a critical 500 kilovolt (kV) transformer substation, demonstrated that such facilities face real and potentially sophisticated threats.<sup>6</sup> The September 2016 rifle attack on a 69 kV transformer substation in Utah—which reportedly left 13,000 rural customers without power for up to eight hours—showed that similar incidents could occur almost anywhere on the grid.<sup>7</sup> A successful cyberattack on Ukraine’s power grid in 2015, which was reportedly attributed to Russian hackers, showed that foreign entities could view power grids as attractive targets.<sup>8</sup> A 2017 report from the National Academy of Sciences concludes: “While to date there have been only minor attacks on the power system in the United States, large-scale physical destruction of key parts of the power system by terrorists is a real danger. Some physical attacks could cause disruption in system operations that last for weeks or months.”<sup>9</sup>

The persistent threat environment has been changing the perception of physical threats among power grid owners and operators. For example, surveys of electric utility employees show that their physical (and cyber) security concerns are growing.<sup>10</sup> Exelon Corporation, one of the nation’s largest utility holding companies, stated in its 2016 annual report:

Threat sources continue to seek to exploit potential vulnerabilities in the electric...utility industry associated with protection of sensitive and confidential information, grid infrastructure and other energy infrastructures, and such attacks and disruptions, both physical and cyber, are becoming increasingly sophisticated and dynamic....The risk of these system-related events and security breaches occurring continues to intensify....<sup>11</sup>

Xcel Energy, another major utility owner, likewise states in its 2016 annual report:

<sup>5</sup> See, for example: National Research Council, *Terrorism and the Electric Power Delivery System*, 2012 and Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, June 1990.

<sup>6</sup> RTO Insider, “Substation Saboteurs ‘No Amateurs,’” April 2, 2014, <http://www.rtoinsider.com/pjm-grid2020-1113-03/>.

<sup>7</sup> Pat Reavy, “Power Company Offers Rare \$50K Reward for Information on Vandalism,” *Deseret News*, September 29, 2016. A substation rated at 69 kilovolts is not considered a “high voltage” transmission asset, although it may still serve large numbers of customers.

<sup>8</sup> Jim Finkle, “U.S. Firm Blames Russian ‘Sandworm’ Hackers for Ukraine Outage,” *Reuters*, January 7, 2016. The attack reportedly cut power to 80,000 customers for about six hours.

<sup>9</sup> National Academy of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation’s Electricity System*, 2017, p. 65, <https://doi.org/10.17226/24836>.

<sup>10</sup> Utility DIVE, *2017 State of the Electric Utility Survey*, April 10, 2017, [https://s3.amazonaws.com/dive\\_assets/rllsys/SEU\\_2017.pdf](https://s3.amazonaws.com/dive_assets/rllsys/SEU_2017.pdf).

<sup>11</sup> Exelon Corporation, *Annual Report Pursuant to Section 13 or 15(d) of the Securities and Exchange Act of 1934 for the Fiscal Year Ended December 31, 2016*, Form 10-K, February 13, 2017, p. 63.



Our generation plants, fuel storage facilities, transmission and distribution facilities and information systems may be targets of terrorist activities... The potential for terrorism has subjected our operations to increased risks and could have a material effect on our business.<sup>12</sup>

Accordingly, electricity sector-wide security exercises conducted by NERC have simulated attacks on power grid critical assets combining both cyber and physical dimensions.<sup>13</sup> These exercises are further discussed later in this report.

## NERC's Physical Security Standards

On March 7, 2014, FERC ordered NERC to submit proposed reliability standards requiring transmission owners meeting certain criteria “to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation” of the power grid.<sup>14</sup> In its order FERC stated that physical security standards were necessary because “the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks.”<sup>15</sup> According to the FERC order, the new reliability standards were to require transmission owners or operators to perform a risk assessment of their systems to identify “critical facilities,” evaluate the potential threats and vulnerabilities to those identified facilities, and develop and implement a security plan designed to protect against physical attacks on those identified critical facilities.<sup>16</sup> The order required that each of these steps be verified by NERC or another third party qualified to review them.

On May 23, 2014, NERC filed with FERC its proposal for mandatory physical security standards.<sup>17</sup> On November 20, 2014, FERC approved the proposed standard, with minor changes, as NERC's new *Physical Security Reliability Standard* (CIP-014-1).<sup>18</sup> Following publication in the *Federal Register*, FERC's order approving the standard became effective on January 26, 2015.<sup>19</sup> FERC approved a revised version of the standard (CIP-014-2) on July 14, 2015.<sup>20</sup> Required compliance for the standard began on October 1, 2015 with completion of the final parts required by November 24, 2016 for all applicable entities.

<sup>12</sup> Excel Energy, Inc. *Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2016*, Form 10-K, p. 44.

<sup>13</sup> North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014 and *Grid Security Exercise, GridEx III Report*, March 2016; Scott Heffentrager, PJM Interconnection, “GridEx IV Summary,” slide presentation, November 27, 2017, <http://www.pjm.com/-/media/committees-groups/committees/mc/20171127-webinar/20171127-item-04-2017-gridex-iv-summary.ashx>.

<sup>14</sup> Federal Energy Regulatory Commission (hereinafter, FERC), *Reliability Standards for Physical Security Measures*, Order Directing Filing of Standards, Docket No. RD14-6-000, March 7, 2014, p.1, <http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf>.

<sup>15</sup> FERC, March 7, 2014, p. 2.

<sup>16</sup> FERC, March 7, 2014, pp. 3-4.

<sup>17</sup> NERC, Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-014-1, May 23, 2014, <http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Physical%20Security%20CIP-014-1.pdf>.

<sup>18</sup> FERC, “Physical Security Reliability Standard,” Docket No. RM14-15-000, Order No. 802, November 20, 2014.

<sup>19</sup> NERC, “Physical Security Reliability Standard Implementation,” January 16, 2015, [http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20\(Agenda%20Excerpt\).pdf](http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20(Agenda%20Excerpt).pdf).

<sup>20</sup> FERC, letter order to the North American Electric Reliability Corporation, Docket No. RD-15-4-000, July 14, 2015, [http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Letter\\_Order\\_CIP-014\\_20150714\\_RD15-4.pdf](http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Letter_Order_CIP-014_20150714_RD15-4.pdf).

## Physical Security Standard Requirements

The stated purpose of NERC’s physical security reliability standard is “to identify and protect transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or cascading within an interconnection.”<sup>21</sup> It applies to transmission owners with assets operating at 500 kV or higher as well as owners with substations operating between 200 kV and 499 kV if they meet certain interconnection or load-carrying criteria.<sup>22</sup> The standard, generally referred to as “CIP-014,” consists of six principal requirements (R1-R6), summarized as follows:

- R1. Risk assessments by transmission owners to identify critical transmission facilities;
- R2. Independent third party verification of risk assessments conducted under R1;
- R3. Requirement for transmission owners with critical facilities identified under R1 but not under their operational control to notify the transmission operator of these facilities;<sup>23</sup>
- R4. Mandatory threat and vulnerability assessments for critical facilities conducted by transmission owners and operators;
- R5. Development, documentation, and implementation of physical security plans to protect critical facilities; and
- R6. Independent third party review of the threat and vulnerability assessments performed under R4 and security plans developed under R5.<sup>24</sup>

The standard also lays out a process for compliance monitoring and assessment including audits, self-certifications, spot checking, violation investigations, self-reporting, and handling complaints.<sup>25</sup> The new standard is enforced by NERC or another Regional Entity under a penalty review policy for mandatory reliability standards approved by FERC subject to the Commission’s enforcement authority and oversight under the Energy Policy Act of 2005 (P.L. 109-58).<sup>26</sup> Monitoring of compliance with the standard is further discussed below.

## Federal Oversight and Support

Three entities play key roles in standards oversight and implementation support for bulk power physical security. NERC and FERC directly oversee implementation of the CIP-014 standards, while the Department of Energy (DOE) plays a supporting role in helping bulk power asset owners to protect their critical assets.

<sup>21</sup> NERC, *CIP-014-2 – Physical Security*, printed December 5, 2017, p. 1, available at [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical%20Security&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical%20Security&jurisdiction=United%20States). (Hereinafter CIP-014-2). This report uses the terms “critical assets” and “critical substations” to mean “critical transmission stations and transmission substations” as defined under the CIP-014 standard.

<sup>22</sup> CIP-014-2.

<sup>23</sup> A regional transmission operator (RTO) administers the transmission grid for multiple transmission owners in a specified region in accordance with FERC Order No. 2000. RTOs and independent system operators (ISOs) are defined in Section 3 of the Federal Power Act (16 U.S.C. 796).

<sup>24</sup> CIP-014-2, pp. 3-6.

<sup>25</sup> CIP-014-2, p.8.

<sup>26</sup> FERC, *Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672*, Docket Nos. AD08-6-000 and RM05-30-002, April 17, 2008.

## NERC's Implementation Oversight

As stated above, with oversight by FERC, NERC has the authority to develop, oversee, and enforce implementation of the CIP-014 physical security standard.<sup>27</sup> NERC carries out these functions together with the eight Regional Entities (e.g., Midwest Reliability Organization) with which NERC has agreements to delegate its authority to monitor and enforce reliability standards compliance.<sup>28</sup> Collectively, NERC and the Regional Entities comprise the Electric Reliability Organization (ERO) Enterprise.

In general, NERC employs a risk-based framework to monitor compliance of all its grid reliability standards on the belief that monitoring and enforcement must be “right-sized” based on considerations including risk factors and management practices related to detecting, assessing, mitigating, and reporting of noncompliance.<sup>29</sup>

As reliability risk is not the same for all registered entities, the Framework examines [bulk power system] risk of registered entities both collectively and individually, to determine the most appropriate [Compliance Monitoring and Enforcement Program] tool to use when monitoring a registered entity's compliance with NERC Reliability Standards. The Framework also promotes an examination into how registered entities operate and tailor compliance monitoring focus to areas that pose the greatest risk to [bulk power system] reliability.<sup>30</sup>

NERC's approach offers flexibility in both the frequency and type of compliance monitoring (e.g., offsite or onsite audits, spot checks, or self-certifications) applied to an entity under a particular standard based on its particular level of reliability risk.<sup>31</sup> To support its compliance approach, NERC may conduct various activities, such as publishing guidance documents, providing training, and conducting outreach, “to promote transparency and confidence” in the utility industry's implementation of a standard.<sup>32</sup>

In monitoring compliance of the CIP-014 standard, NERC's focus in 2015 and 2016 was on the standards' requirements to identify critical transmission stations and substations (Requirements R1 and R2), ensuring that this identification was “appropriate and risk-informed.”<sup>33</sup> NERC required covered entities to self-certify with respect to: risk-assessment, identifying critical assets, and third party verification. NERC also conducted voluntary outreach through on-site visits with 19 covered entities to discuss security measures and CIP-014 implementation challenges.<sup>34</sup> In

---

<sup>27</sup> NERC's authorities to monitor compliance with its reliability standards and impose financial penalties are found in FERC regulations at 18 C.F.R. 39.7.

<sup>28</sup> See NERC, “Key Players,” web page, March 13, 2018, <http://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>.

<sup>29</sup> NERC, *Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program*, September 5, 2014, p. iv.

<sup>30</sup> NERC, *2017 ERO Enterprise Compliance Monitoring and Enforcement Implementation Plan, Version 2.5*, May 2017, p. 3.

<sup>31</sup> NERC, May 2017, p. 3.

<sup>32</sup> NERC, “Physical Security Reliability Standard Implementation,” January 16, 2015, p. 3, [http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20\(Agenda%20Excerpt\).pdf](http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20(Agenda%20Excerpt).pdf)

<sup>33</sup> NERC, May 2017, p. 16.

<sup>34</sup> NERC, *2016 ERO Enterprise Compliance Monitoring and Enforcement Program Annual Report*, February 8, 2017, p. 18, <http://www.nerc.com/pa/comp/CE/Compliance%20Violation%20Statistics/2016%20Annual%20CMEP%20Report.pdf>.

cases where there have been discrepancies between utility-generated critical asset lists and critical assets identified by the independent third parties, NERC has required the covered entities to provide further information and explanation to address the discrepancy. NERC has also been conducting audits of entities which have identified more, or fewer, critical substations as a percentage of all their substations than is typical.<sup>35</sup> The detailed findings of NERC's compliance activities are not publically disclosed due to the confidential nature of security information. However, NERC stated that, based on observations in 2016, the utility industry was "making progress towards effective implementation of and compliance with CIP-014-2."<sup>36</sup> A NERC presentation about its voluntary and informal site visits reported "remarkable progress" on physical security among 19 asset owners visited as of February 2016.<sup>37</sup>

In 2017, NERC increased its focus on the scope of utility security plans (R5), including their timelines for implementing security measures and the utility industry's overall progress in implementing CIP-014. The ERO Enterprise has prioritized auditing the quality of covered entities' risk management plans. In the second quarter of 2017, compliance audit staff were provided with guidance and training on bulk power physical security best practices as a reference for evaluating the physical security measures implemented by the covered entities.<sup>38</sup>

The ERO Enterprise expects to complete audits of the largest entities within three years of the effective date of CIP-014. As of February 2018, NERC had conducted compliance audits of approximately 45% of the covered entities with critical transmission stations and substations as defined under CIP-014. NERC had also audited over 30% of entities that did not identify critical assets after applying the CIP-014 criteria (under R1). NERC staff expects to have audited approximately 70% of the entities with CIP-014 critical assets by the end of 2018.<sup>39</sup> According to its stated schedule, NERC would audit the remaining entities in 2019. Subsequent monitoring and enforcement will focus more heavily on implementation of measures in the grid security plans.

According to NERC, the audits completed to date have not uncovered any major compliance failures, and NERC has been "encouraged" by security measures that utilities have put in place so far.<sup>40</sup> NERC has found no serious risk violations of the CIP-014 standard. Of 19 noncompliance issues identified, 8 were found to be "minimal" or "moderate" risk, with 2 warranting a financial penalty. The remaining 11 noncompliance issues are under review.<sup>41</sup>

## Electricity Information Sharing and Analysis Center

In addition to its standards activities, NERC also supports security of the electric power sector as the operator of the Electricity Information Sharing and Analysis Center (E-ISAC). Established in

<sup>35</sup> NERC, Staff meeting with CRS analysts, Washington, DC, December 7, 2017.

<sup>36</sup> NERC, May 2017, p. 16.

<sup>37</sup> Carl Herron, NERC, "CIP-014-02 Physical Security Site Visits," slide presentation, April 14, 2016, [https://www.frc.com/Compliance/EducationalMaterials/Educational%20Materials/Workshops%20-%20Workshop%20Event%20Materials/2016-04%20-%20OP%20Spring%20Compliance%20Workshop%20\(April%202012-14\)/7.%20CIP-014-2%20Physical%20Security%20Site%20Visits.pdf](https://www.frc.com/Compliance/EducationalMaterials/Educational%20Materials/Workshops%20-%20Workshop%20Event%20Materials/2016-04%20-%20OP%20Spring%20Compliance%20Workshop%20(April%202012-14)/7.%20CIP-014-2%20Physical%20Security%20Site%20Visits.pdf).

<sup>38</sup> NERC, *Compliance Monitoring and Enforcement Program Quarterly Report, Q2 2017*, August 9, 2017, p. 8, <http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/Compliance%20Committee%20Open%20Meeting%20-%20August%209%202017.pdf>.

<sup>39</sup> NERC, email to CRS, February 14, 2018.

<sup>40</sup> NERC, December 7, 2017.

<sup>41</sup> NERC, February 14, 2018.

1998, the E-ISAC is the electricity sector's primary communications channel for security-related information, situational awareness, incident management, and coordination.<sup>42</sup> Among its key responsibilities, the E-ISAC gathers and analyzes security data, shares it with stakeholders, and communicates security risk mitigation strategies.<sup>43</sup> Bulk power entities are required to report physical security events to the E-ISAC under NERC's Event Reporting Reliability Standard (EOP-004), which was approved by FERC in 2013 and revised in 2015.<sup>44</sup>

Although operated by NERC, the E-ISAC is independent and organizationally separate from NERC's standards enforcement functions; information shared by utilities with the E-ISAC is not passed on to NERC compliance staff.<sup>45</sup> Nonetheless, the E-ISAC has played a role in facilitating industry understanding of physical security best practices. For example, the E-ISAC has added significant physical security threats and tactics to the NERC's biennial GridEx security exercises (discussed later in this report). In 2015, the E-ISAC also established a Physical Security Advisory Group, which includes industry physical security professionals, outside experts, and representatives from DOE and the Department of Homeland Security (DHS), to assist in the analysis of physical security threats and advise asset owners on physical threat mitigation. Through these efforts, the E-ISAC developed and ratified a design basis threat for the electric sector in December 2015.<sup>46</sup> The E-ISAC also has hosted two threat workshops, with plans for more.<sup>47</sup> Thus, while the E-ISAC has had no role in enforcing the CIP-014 standards, the security risk and mitigation information it develops and promulgates support the activities of bulk power asset owners complying with the standards.

## FERC Oversight

As the agency with general statutory authority over grid reliability, and the agency which ordered and approved NERC's CIP-014 standard, the Federal Energy Regulatory Commission also oversees implementation of the standard. In carrying out this oversight, FERC relies primarily on annual compliance reporting by NERC.<sup>48</sup> However the commission also conducts some independent compliance activities, and it also conducts some compliance activities in cooperation with NERC. For example, during the initial rollout of the CIP-014 standard in 2016, FERC staff coordinated with NERC staff in support of on-site visits to the covered entities discussed above.<sup>49</sup>

In its order approving CIP-014-01, the commission stated that NERC staff would submit to both the NERC Board of Trustees and FERC a report following implementation of requirements R1,

<sup>42</sup> ISACs for critical infrastructure sectors were established under Presidential Decision Directive 63, May 22, 1998. NERC operates the E-ISAC in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC). The ESCC, established in 2004 by companies in the electric power industry, coordinates policy-related activities involving the reliability and resilience of the sector, including physical and cyber infrastructure.

<sup>43</sup> NERC, *Understanding Your E-ISAC*, June 2016, p. 3.

<sup>44</sup> NERC, "EOP-004-3—Event Reporting," 2015, <http://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-3.pdf>.

<sup>45</sup> NERC, June 2016, p. 3.

<sup>46</sup> NERC, *State of Reliability 2016*, May 2016, p. 7.

<sup>47</sup> NERC, *State of Reliability 2017*, June 2017, p. 62.

<sup>48</sup> FERC, *Order on Electric Reliability Organization Reliability Assurance Initiative and Requiring Compliance Filing*, Docket No. RR15-2-000, p. 11, February 19, 2015, [http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/FERC\\_Order\\_Approving\\_Risk-Based\\_CMEP.pdf](http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/FERC_Order_Approving_Risk-Based_CMEP.pdf).

<sup>49</sup> NERC, May 2017, p. 16.



R2, and R3 about the scope, number, and characteristics of facilities identified as critical.<sup>50</sup> The order stated that

Based on the results reported by NERC, we expect Commission staff to audit a representative number of applicable entities to ensure compliance with Reliability Standard CIP-014-1. Depending on the audit findings, the Commission will determine if there is a need for any further action by the Commission including, but not limited to, directing NERC to develop modifications to Reliability Standard CIP-014-1 to provide greater specificity to the methodology for determining critical facilities.<sup>51</sup>

As of November 2, 2017, FERC had completed two audits of critical assets identified by covered entities (R1) and was in the process of conducting a third. These audits have involved technical review of utility regulatory documents by FERC engineers. According to FERC staff, the initial audits identified one issue of concern related to the interpretation of specific language in the standard regarding asset criticality.<sup>52</sup> In addition to NERC's annual reports, FERC receives from NERC periodic Notices of Penalty (NOP) to regulated entities for reliability standards violations. As of November 30, 2017, FERC received NOPs for two violations (apparently at the same utility) of the CIP-014 standard.<sup>53</sup>

## DOE Initiatives

Presidential Decision Directive 63 (PDD-63), issued during the Clinton Administration in 1998, established national policy for critical infrastructure protection from both physical and cyber threats.<sup>54</sup> PDD-63 established 15 critical infrastructure sectors. The Department of Energy was assigned responsibility for (1) the electric power, and (2) the oil and natural gas production and storage sectors. The George W. Bush Administration built on the work of PDD-63, superseding it in 2003 with Homeland Security Presidential Directive 7 (HSPD-7) on "Critical Infrastructure Identification, Prioritization, and Protection."<sup>55</sup> HSPD-7 again assigned to DOE (as a Sector-Specific Agency) responsibility for the energy sector—including electric power—as well as responsibility for being the federal coordinator for all critical infrastructure protection efforts.<sup>56</sup> The Obama Administration superseded HSPD-7 with Presidential Policy Directive 21 (PPD-21) on "Critical Infrastructure Security and Resilience" in 2013.<sup>57</sup> PPD-21 retained the Sector-Specific Agencies (SSAs) from HSPD-7, with DOE continuing as the SSA for the energy sector. Thus, DOE has had a supportive role in helping utilities to protect bulk power critical assets over the last two decades.

<sup>50</sup> FERC, *Physical Security Reliability Standard*, Docket No. RM14-15-000, Order No. 802, November 20, 2014, p. 23, <http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Final%20Rule%20on%20CIP-014-1.pdf>.

<sup>51</sup> FERC, Order No. 802, p. 24.

<sup>52</sup> FERC, Staff meeting with CRS analysts, Washington, D.C., November 2, 2017.

<sup>53</sup> NERC, *Enforcement and Mitigation*, "Searchable NOP Spreadsheet," web page, accessed December 12, 2017, <http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx>.

<sup>54</sup> National Security Council and National Security Council Records Management Office, "PDD-63—Critical Infrastructure Protection," *Clinton Digital Library*, May 20, 1998.

<sup>55</sup> George W. Bush White House Archives, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive/HSPD-7, December 17, 2003.

<sup>56</sup> For details about the roles of Sector-Specific Agencies, see Department of Homeland Security, "Sector-Specific Agencies," web page, July 11, 2017, <https://www.dhs.gov/sector-specific-agencies>.

<sup>57</sup> Barack H. Obama White House Archives, "Critical Infrastructure Security and Resilience," Presidential Policy Directive-21, February 12, 2013.

Until recently, DOE's power grid security activities were led by its Office of Electricity Delivery and Energy Reliability (OE) within the Office of the Under Secretary for Science and Energy. A 2008 OE report stated that "OE's mission is to advance technology—in partnership with industry, government, academia, and the public—to meet America's need for a reliable, efficient, and resilient electric power grid."<sup>58</sup> Although the office was primarily focused on grid cybersecurity, it did conduct activities related to power grid physical security, including analysis of large power transformer security, a substation security awareness campaign, and efforts to support and coordinate research and development for physical security.<sup>59</sup> On February 14, 2018, DOE announced that the Secretary of Energy was establishing a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to be led by an Assistant Secretary with responsibilities to help protect energy infrastructure from "from cyber threats, physical attack and natural disaster."<sup>60</sup> How this reorganization will affect DOE's activities in bulk power physical security remains to be seen.

## Observed Changes in Bulk Power Physical Security

Most grid security analysts consider the 2013 Metcalf substation attack to have been the "wake up call" which both changed electric sector attitudes toward grid physical security and motivated the promulgation of NERC's physical security regulations. Since that time, there have been a number of apparent changes within the electricity sector related to increasing bulk power physical security. It is not clear whether these changes have been driven more by changes in utility perceptions of grid threats or by NERC's mandatory security standards. Furthermore, there is currently no comprehensive accounting of changes in physical security throughout the sector. Nonetheless, anecdotal information in the public domain suggests that such changes may be significant and widespread. They are discussed in the following sections.

### Corporate Structure Supporting Physical Security

One criticism that arose in the wake of the Metcalf attack was that physical security management at Pacific Gas and Electric Company (PG&E, the Metcalf substation's owner) and at other utilities was not a centrally organized or well-supported function in corporate management. This lack of support limited the influence of security managers in corporate planning and financial decisions.<sup>61</sup> However, it appears that many utilities have been reconfiguring and elevating physical security functions within their corporate structures. For example, owners of transmission assets such as PG&E, American Electric Power, and Xcel Energy have appointed Chief Security Officers at senior levels responsible for managing both physical and cyber security risks company-wide.<sup>62</sup>

<sup>58</sup> Department of Energy, Office of Electricity Delivery and Energy Reliability (Hereinafter OE), *National SCADA Test Bed Program, Multi-Year Plan FY2008-2013*, January 2008, p. 7.

<sup>59</sup> Department of Energy, Energy Sector-Specific Plan, 2015, pp. 16, 27. For discussion of OE's cybersecurity activities, see CRS Report R44939, *Cybersecurity for Energy Delivery Systems: DOE Programs*, by Paul W. Parfomak, Chris Jaikaran, and Richard J. Campbell.

<sup>60</sup> U.S. Department of Energy, "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response," press release, February 14, 2018.

<sup>61</sup> See, for example: Tony Kovalesski, Liz Wagner, and Mark Villarreal, "Internal Memo Reveals PG&E Years Away from Substation Security," *NBC Bay Area*, April 5, 2106, <https://www.nbcbayarea.com/investigations/Internal-Memo-Reveals-PGE-Years-Away-from-Substation-Security-303833811.html>.

<sup>62</sup> PG&E Corp., "Bernard A. Cowens," web page, January 9, 2017, <http://www.pgecorp.com/corp/about-us/officers/> (continued...)

The senior security professional, typically at the vice president or director level, now has direct access to the [Chief Executive Officer] and company boards of trustees, often to supply situational awareness of physical and cybersecurity issues.... The electricity industry is quickly moving away from security as an “addition duty”.... [M]ost utilities today have dedicated security departments committed to the protection of company assets and personnel.<sup>63</sup>

Utilities are also centralizing and bolstering their physical security capabilities at the operational level. Between 2014 and 2017, for example, Xcel Energy consolidated and grew its staffing for the “Chief Security Officer class of services” from 47 to 63 employees.<sup>64</sup> According to the company’s regulatory filings,

the increase in average staffing levels.... was due to the need to correct a lack of resources to ensure adequate headcount to provide essential cyber and physical Enterprise Security services for Xcel Energy.... This increase in staffing demonstrates the emerging need that led to a stand-alone organization (i.e., the Chief Security Officer) to focus on Cyber Operations, Enterprise Resilience, Physical Security and Security Governance.<sup>65</sup>

Likewise, in response to the Metcalf attack, Dominion Energy established “a true cross-functional team with more than 100 people representing the entire Dominion organization,” to develop and implement a more comprehensive substation security program.<sup>66</sup> Such efforts appear to extend to major publicly owned utilities as well. For example, according to the head of the Western Area Power Administration (WAPA), one of four federal power marketing administrations,

WAPA’s approach to physical security.... began in 2013 with the consolidation of our Office of Security and Emergency Management across our five regions and the implementation of a sophisticated risk-based program in analyzing the threats and vulnerabilities to our substations.<sup>67</sup>

The Tennessee Valley Authority (TVA), which operates federally-owned hydroelectric and nuclear generation and associated transmission assets, recently closed a job posting for eight entry-level Inspectors, each to be “trained as a physical security specialist” to provide “comprehensive security services, including assessments of facilities to identify credible threats, and implementation and testing of countermeasures to mitigate risks.”<sup>68</sup>

---

(...continued)

company/bernard-cowens.page; American Electric Power, “AEP Names Partlow Vice President & Chief Security Officer,” press release, August 25, 2015; Xcel Energy, *Application of Southwestern Public Service Company for Authority to Change Rates*, Direct Testimony of Stephen J. Brown, filing with the Public Utility Commission of Texas, August 21, 2017, <https://www.xcelenergy.com/staticfiles/xcel-responsive/Company/Rates%20&%20Regulations/Rate%20Cases/Brown-RR-Direct.pdf>.

<sup>63</sup> Brian Harrell, “The Modern Look of a Utility’s Chief Security Officer,” *CSO*, August 4, 2016, <https://www.csoonline.com/article/3101474/leadership-management/the-modern-look-of-a-utilitys-chief-security-officer.html>.

<sup>64</sup> Xcel Energy, *Application of Southwestern Public Service Company for Authority to Change Rates*, Update Testimony of Stephen J. Brown, September 27, 2017, p. 10, <https://www.xcelenergy.com/staticfiles/xcel-responsive/Company/Rates%20&%20Regulations/Rate%20Cases/13%20-%20BrownRRUpdate.pdf>.

<sup>65</sup> Xcel Energy, August 21, 2017, p. 26.

<sup>66</sup> Bob McGuire, et al., “Substation Security Is More Than Just a Fence,” *T&D World*, September 28, 2015.

<sup>67</sup> Mark A. Gabriel, Administrator and Chief Executive Officer, Western Area Power Administration, “Physical and Cyber Threats,” *T&D World*, May 8, 2017. Power Marketing Administrations (PMAs) operate electric transmission systems and sell power generated by federally-owned hydroelectric dams across much of the United States.

<sup>68</sup> Tennessee Valley Authority, “Inspector I – 507038,” job posting, *Linked-in JOBS*, web page, posted January 17, 2018, accessed February 1, 2018, <https://www.linkedin.com/jobs/view/inspector-i-507038-at-tennessee-valley-> (continued...)

Some transmission owners are also specifically increasing their in-house intelligence capabilities in physical security, including recent postings for positions such as “Security Intelligence Specialist” and “Director—Corp Security Info & Intelligence.”<sup>69</sup> While the examples above are anecdotal, they would be consistent with what may be a trend among key grid owners to make physical security a better-organized and more influential corporate function. Not all utilities may be implementing such organizational changes, however.

## Physical Security in Long-Term Transmission Planning

Since NERC promulgated the CIP-014 standards, some utilities have begun to put a greater emphasis on bulk power physical security as a design consideration in long-term transmission system planning. This approach aligns with the California Public Utilities Commission’s recommendation in its 2018 report that, “there should be an emphasis on incorporating a menu of physical security strategies [into] any substation from the time of its inception.”<sup>70</sup> For example, Public Service Enterprise Group’s transmission planning criteria for its Long Island system in New York discusses the use of power system simulation tools for “various transmission system security and reliability studies.”<sup>71</sup> Commonwealth Edison’s transmission planning criteria includes a separate section on “security criteria” for system design which considers “severe low probability outage combinations” and seeks “to avoid cascading outages, instability, or widespread blackout.”<sup>72</sup> Such criteria could apply to both natural and man-made outages, but they are consistent with, and readily applied to, design considerations for enhanced physical security. American Electric Power (AEP) also has incorporated asset criticality as a design criterion in its transmission planning.

As a result of the revised NERC CIP standards, AEP now classifies all of its bulk electric system facilities based on the critical nature of the equipment to determine the level of security needed. This approach allows us to design security controls directly into new infrastructure from the start, building the costs into capital projects as needed. It also allows us to be more proactive with new and existing infrastructure while balancing risks with mitigation solutions.<sup>73</sup>

In its plans for a 2018 reliability-related upgrade at one its substations, Vermont Electric Power Company states that it “will also take the opportunity to make improvements to the physical security” of the substation.<sup>74</sup> According to NERC officials, based on security criteria, some

(...continued)

authority-578188690.

<sup>69</sup> American Transmission Company, “Security Intelligence Specialist,” job listing on *LinkedIn*, posted March 6, 2017, <https://www.linkedin.com/jobs/view/security-intelligence-specialist-at-american-transmission-552328921>; Avangrid, “Director—Corp Security Info & Intelligence,” job listing on *Glassdoor.com*, posted January 3, 2018, [https://www.glassdoor.com/job-listing/director-corp-security-info-intelligence-avangrid-JV\\_IC1148470\\_KO0,40\\_KE41,49.htm?jl=2630675613&utm\\_source=google\\_jobs&utm\\_medium=organic](https://www.glassdoor.com/job-listing/director-corp-security-info-intelligence-avangrid-JV_IC1148470_KO0,40_KE41,49.htm?jl=2630675613&utm_source=google_jobs&utm_medium=organic).

<sup>70</sup> CPUC, January 2018, p. 8.

<sup>71</sup> PSEG Long Island, “Transmission Planning Criteria,” accessed January 10, 2018, p. 5, <https://www.psegliny.com/files.cfm/TransmissionPlanningCriteria.pdf>.

<sup>72</sup> Commonwealth Edison Co., “Transmission Planning Criteria,” February 10, 2017, p. 10, <https://www.pjm.com/-/media/planning/planning-criteria/commonwealth-edison-planning-criteria.ashx?la=en>

<sup>73</sup> American Electric Power Corp., *2017 AEP Corporate Accountability Report*, “Cyber and Physical Security,” web page, May 25, 2017, <http://www.aepsustainability.com/about/security/cyber.aspx>.

<sup>74</sup> Vermont Electric Power Company, “East Avenue & Queen City Substation Improvement Project,” web page, accessed February 1, 2018, <https://www.velco.com/our-work/projects/project-east-avenue-queen-city-substation-improvement-project>.

utilities also have begun to consider new transmission interconnections not only to increase line capacity for bulk power flows, but also to reduce the criticality of particular transformer substations in congested areas by providing more transmission paths around them.<sup>75</sup>

## New Security Products and Services

As utilities have devoted greater organizational and financial resources towards power grid physical security, industry vendors have been offering more physical security products and services to meet sector demand. As one utility services company has observed, “we can expect plenty of innovation as manufacturers see new markets due to the new standards for physical security of critical substations.”<sup>76</sup> These offerings range from analytical services for security planning to physical products to harden physical assets. A comprehensive survey of such offerings is beyond the scope of this report, but the following examples illustrate the kinds of products now commercially available in the bulk power physical security market.

- **Security Program Planning and Implementation.** Engineering and security consulting firms have developed customizable programs specifically for power grid physical security review, planning, analysis, and implementation in compliance with the CIP-014 standards and utility-specific requirements.<sup>77</sup>
- **Anti-Intrusion Products.** Vendors have been marketing existing intrusion-related products specifically for use at bulk power critical facilities. These products include visual, acoustic, thermal radar, and electromagnetic systems for facility monitoring, intrusion detection, and response.<sup>78</sup>
- **Hardened Transformers and Components.** At least two major manufacturers have been marketing bulk power transformers with integrated ballistic shielding, or customizable plates to shield existing transformers.<sup>79</sup> Smaller manufacturers have also begun marketing hardened transformer components, such as composite bushings, for new and retrofit substation applications.<sup>80</sup>
- **Substation Perimeter Shielding.** A number of vendors have been marketing perimeter fencing and wall products specifically for visual and physical shielding of bulk power substations.<sup>81</sup> Most of these products are designed specifically to protect against rifle attacks such as the Metcalf attack.

<sup>75</sup> NERC, December 7, 2017.

<sup>76</sup> Southwire Company, “Protecting the Grid,” *T&D World*, sponsored content, May 15, 2017.

<sup>77</sup> See, for example: Burns & McDonnell, “Station Defender,” web page, January 30, 2018, <https://info.burnsmcd.com/station-defender/project-delivery>; Corporate Risk Solutions, “Physical Security,” web page, January 30, 2018, <https://corprisk.net/physical-security/>.

<sup>78</sup> See, for example: “How VTI Security Protected an Electrical Substation With a Radar-Thermal Imaging Solution,” *Security Sales & Integration*, September 20, 2017, <https://www.securitysales.com/in-depth/vti-security-radar-thermal-imaging-solution/>; and i2c Technologies, Ltd., “Power Substation Protection,” marketing brochure, May 2017, <http://www.i2ctech.com/wp-content/uploads/2017/05/2509-i2cTech-CMYK.pdf>.

<sup>79</sup> See, for example: Siemens AG, “First Bullet Resistant Retrofit Ordered for a Transformer,” press release, accessed January 28, 2018, <https://www.siemens.com/global/en/home/products/energy/references/first-bullet-resistant-retrofit-ordered-for-a-transformer.html>.

<sup>80</sup> Mike Sheppard and Saqib Saeed, “Bullet and Weather Concerns Driver of Retrofits in US Market,” Power Technology Research LLC, October 26, 2017, <https://powertechresearch.com/bullet-and-weather-concerns-driver-of-retrofits-in-us-market/>.

<sup>81</sup> See for example: Oldcastle, Inc., “How Precast Substation Walls Increase Power Grid Security,” web page, <https://www.buildingsolutions.com/industry-insights/how-precast-substation-walls-increase-power-grid-security>; (continued...)



Although new physical security products and services are being marketed in the utility sector, there is no comprehensive source of data about their sales to bulk power asset owners. Simply because vendors are marketing products does not mean that many utilities are buying them. For example, as of October 2017, Siemens Corp. had announced only one commercial order for its new transformer ballistic shielding retrofit product.<sup>82</sup> Thus, the overall impact of such offerings on the sector cannot be qualified reliably. Additional discussion of physical security spending is in the following section.

## Capital Investment in Physical Security

Major changes in power grid operational expenses and capital investment are generally slow to occur. In privately owned utilities, significant changes in spending and plans for new capital projects may need to go through a number of rigorous screens, including power network modeling, a corporate capital allocation process, a regulatory approval process, and a procurement process. Publicly owned utilities may need approval from cooperative boards, or municipal or federal officials. This combination of requirements can take years to complete. Consequently, many significant operating expenditures or capital investments for physical security identified in security plans under CIP-014 may still be working their way through utility budgets and implementation. For example, in a 2016 rate filing, Southern California Edison stated that it planned to make physical security improvements at approximately 24 facilities in 2015-2017 and proposed to upgrade 8 substations per year from 2016 through 2020.<sup>83</sup> Likewise, in its 2016 annual report, Dominion Resources' timeline for power grid capital investment in "Physical Security" runs to 2021.<sup>84</sup>

Notwithstanding the potential length of time it may take for some security projects to be approved and implemented, there are indications in the public record that bulk power asset owners have already been spending more on new physical security measures. In its December 2016 report, the Edison Electric Institute stated that "primary factors driving transmission investment between 2015 and 2019" included "system hardening and resiliency to minimize adverse catastrophic events" and "improvements to comply with evolving transmission reliability and security compliance standards."<sup>85</sup> In its January 2018 white paper, the California Public Utilities Commission (CPUC) reports that investor-owned utilities under its jurisdiction "already ... have sought approval for tens of millions of dollars in General Rate Case funding to ensure physical security."<sup>86</sup> The following examples illustrate the types of physical security projects and recent spending in publicly available sources.

(...continued)

AFTEC LLC, "Substation Security Walls," web page, 2017, <https://aftec.com/substation-security-walls/>;

<sup>82</sup> Siemens AG, "First Bullet Resistant Retrofit Ordered for a Transformer," press release, October 17, 2017, <https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/energy-management/medium-voltage-power-distribution/2017-10-17-tr-success-bullet-resistant-retrofit-v1-en.pdf>.

<sup>83</sup> Southern California Edison Co., Application Of Southern California Edison Company (U 338E) For Authority To Increase Its Authorized Revenues For Electric Service In 2018, Among Other Things, And To Reflect That Increase In Rates, A.16-09-001, Before the Public Utilities Commission of the State of California, September 1, 2016, [http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/9F664E3F0B77B7E488258195007C8F53/\\$FILE/SCE%20Opening%20Brief%20and%20COS.pdf](http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/9F664E3F0B77B7E488258195007C8F53/$FILE/SCE%20Opening%20Brief%20and%20COS.pdf).

<sup>84</sup> Dominion Resources, Inc., *Energy is Essential*, 2016 Summary Annual Report, 2017, p. 5.

<sup>85</sup> Edison Electric Institute, *Transmission Projects: At A Glance*, December 2016, p. vi.

<sup>86</sup> California Public Utilities Commission (CPUC), *Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699*, January 2018, p. 5.

- In 2017, the Bonneville Power Administration announced stand-alone plans to install security fencing at two high-voltage substations in compliance with NERC's security standards and to "protect critical assets from theft, vandalism, and terrorism."<sup>87</sup>
- In 2017, PPL Electric Utilities reportedly filed for regulatory approval for a \$450,000 expenditure to reconfigure a 500 kV substation in compliance with NERC's CIP-014 physical security standard.<sup>88</sup>
- In 2017 regulatory filings, Vectren (Indiana) described plans to invest \$2.9 million for physical security upgrades at critical substations, including enhanced fencing, access control, video surveillance, and perimeter motion detection.<sup>89</sup>
- According to the Western Area Power Administration, its expenses for physical security "nearly tripled" between 2013 and 2017.<sup>90</sup>

## Utility Participation in Voluntary Security Programs

Although the CIP-014 mandatory physical security standards have only been in effect since 2014, bulk power asset owners have had earlier opportunities to participate in voluntary security initiatives administered by NERC and DHS. Utility participation in these voluntary programs is another indication of overall efforts in the sector to improve critical asset physical security.

## NERC Grid Security Exercises

In 2011, NERC conducted GridEx, the first of an ongoing series of biennial electric sector-wide grid security exercises.<sup>91</sup> The 2011 exercise assessed the readiness of utilities to respond to a cyberattack, strengthened their crisis response, and provided input for internal security program improvements. Although the exercise was focused on a cyberattack, it did involve physical incursions into power grid substations as well as aspects of grid monitoring and recovery that would be relevant to an attack on critical transformers.<sup>92</sup> After the Metcalf attack in 2013, NERC conducted a second, more expansive grid security exercise, GridEx II. The exercise scenario included a cyberattack on the grid coupled with a coordinated physical attack against a subset of transmission and generation assets—including critical transformer substations.<sup>93</sup> NERC conducted GridEx III in 2015, again including a baseline scenario with cyber and physical

<sup>87</sup> Bonneville Power Administration, Categorical Exclusion Determination, "Proposed Action: Covington and Maple Valley Substations Perimeter Security Upgrades," April 27, 2017, [https://www.bpa.gov/efw/Analysis/CategoricalExclusions/cx/20170427\\_Covington-and-Maple-Valley-Substations-Perimeter-Security-Upgrades.pdf](https://www.bpa.gov/efw/Analysis/CategoricalExclusions/cx/20170427_Covington-and-Maple-Valley-Substations-Perimeter-Security-Upgrades.pdf).

<sup>88</sup> Corina Rivera Linares, "PPL Electric Utilities Seeks Approval of Two Projects in Pennsylvania," *Transmission Hub*, PennWell Publishing, May 22, 2017.

<sup>89</sup> Southern Indiana Gas and Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc. IURC Cause No. 44910, filing with the Indiana Utility Regulatory Commission, February 23, 2017, Attachment LKW-2, p. 31, [https://iurc.portal.in.gov/\\_entity/sharepointdocumentlocation/b4477c28-00fa-e611-8104-1458d04e8ff8/bb9c6bba-fd52-45ad-8e64-a444aef13c39?file=44910\\_Vectren%20South\\_No%202\\_Direct%20Testimony%20and%20Attachments\\_Wilson\\_PUBLIC\\_022317.pdf](https://iurc.portal.in.gov/_entity/sharepointdocumentlocation/b4477c28-00fa-e611-8104-1458d04e8ff8/bb9c6bba-fd52-45ad-8e64-a444aef13c39?file=44910_Vectren%20South_No%202_Direct%20Testimony%20and%20Attachments_Wilson_PUBLIC_022317.pdf)

<sup>90</sup> Mark A. Gabriel, May 8, 2017.

<sup>91</sup> NERC's E-ISAC division organizes and administers its GridEx exercises.

<sup>92</sup> North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. i.

<sup>93</sup> NERC, *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.15; Matthew L. Wald, "Attack Ravages Power Grid. (Just a Test.)," *New York Times*, November 14, 2013.

attacks, but also with an option for participants to customize the baseline scenario to meet local objectives.<sup>94</sup> NERC conducted its most recent exercises, GridEx IV, in November 2017.

According to NERC, one indication of progress in bulk power grid security is increasing participation by electricity sector entities in its GridEx exercises. The number of utilities participating in GridEx rose from 49 in 2011 to 166 in 2015.<sup>95</sup> NERC has not yet released participation details for GridEx IV, but the DOE reported that the latest exercise had more participants than in 2015.<sup>96</sup>

## DHS Critical Infrastructure Surveys

The Department of Homeland Security's Protective Security Coordination Division conducts voluntary field assessments of critical infrastructure to identify vulnerabilities, interdependencies, capabilities, and cascading effects of potential terrorist attacks. As part of these efforts, DHS Protective Security Advisors offer voluntary, web-based security surveys of critical facility security using the agency's Infrastructure Survey Tool developed in 2008. The key goals of the surveys are to identify facilities' physical security and security management, identify security gaps, create facility protective and resilience measures indices that can be compared to similar facilities, and track progress toward improving security.<sup>97</sup> According to DHS officials, of more than 6,000 surveys completed since the program began, over 600 have been conducted on electric power facilities—although the timing of these surveys and the specific types of power facilities involved are not reported.<sup>98</sup>

## Legislative Proposals in the 115<sup>th</sup> Congress

Given the relatively recent promulgation of NERC's new physical security standards, bulk power physical security has not been a major legislative focus in the 115<sup>th</sup> Congress. Nonetheless, several bills include provisions intended to enhance bulk power physical security—primarily by establishing new DOE grid security programs rather than by imposing new requirements on FERC or on bulk power asset owners directly. The relevant provisions of these bills, and a related resolution, are summarized below.

- **The Enhancing Grid Security Through Public-Private Partnerships Act** (H.R. 5240) would require DOE to establish a program to facilitate public-private partnerships for electric utility physical security and cybersecurity, among other provisions. Program activities would support voluntary implementation of maturity models, self-assessment, and security auditing; sharing of best practices and data collection in the electric sector; and training and technical assistance to utilities (§2(a)).

<sup>94</sup> NERC, *Grid Security Exercise: GridEx III Report*, March 2016, p. 7.

<sup>95</sup> NERC, March 2016, p. 1.

<sup>96</sup> U.S. Department of Energy, "GridEx IV: Government and Industry Exercise Together to Improve the Response to Grid Security Emergencies," November 21, 2017, <https://energy.gov/articles/gridex-iv-government-and-industry-exercise-together-improve-response-grid-security>.

<sup>97</sup> Department of Homeland Security, "Critical Infrastructure Vulnerability Assessments," web page, April 17, 2017, <https://www.dhs.gov/critical-infrastructure-vulnerability-assessments>.

<sup>98</sup> Daniel Genua, Department of Homeland Security, Presentation at George Mason University, Center for Energy Science and Policy, Grid Security Symposium, Arlington, VA, October 25, 2017, [http://cesp.gmu.edu/wp-content/uploads/2017/10/UNCLASS\\_GMU-Panel-Presentation\\_25Oct2017\\_FINAL.pdf](http://cesp.gmu.edu/wp-content/uploads/2017/10/UNCLASS_GMU-Panel-Presentation_25Oct2017_FINAL.pdf).

- The **Energy Emergency Leadership Act** (H.R. 5174) would amend the Department of Energy Organization Act to include “energy emergency and energy security” to the functions assigned to Assistant Secretaries. These functions would include responsibilities with respect to emerging threats, supply, and emergency planning, among others. They would also include “provision of technical assistance, support, and response capabilities with respect to energy security threats, risks, and incidents” (§2).
- The **Energy and Natural Resources Act of 2017** (S. 1460) would require DOE to develop an advanced energy security program to secure energy networks, including electric transmission and delivery. Eligible activities would include developing “capabilities to identify vulnerabilities and critical components that pose major risks to grid security if destroyed or impaired,” modeling national level impacts from human-made events, developing a physical security maturity model, conducting grid security exercises, conducting research on critical asset hardening, and other related measures (§2002(e)).
- The **Leading Infrastructure for Tomorrow’s America Act** (H.R. 2479) would establish a grant program administered by DOE “to enhance energy security through measures for electricity delivery infrastructure hardening and enhanced resilience and reliability” (§31101(a)).
- The **Advancing Grid Storage Act of 2017** (S. 1851) would establish a competitive grant program for pilot energy storage systems administered by DOE with one objective being to “improve the security of critical infrastructure and emergency response systems” in the electric grid (§5(a)(4)(A)).
- The **Grid Cybersecurity Research and Development Act** (H.R. 4120) would require DOE, together with bulk power asset owners, and in collaboration with the National Laboratories, to “utilize a range of methods, including voluntary vulnerability testing and red team-blue team exercises, to identify vulnerabilities in physical and cyber systems” (§6(a)).
- The **Flexible Grid Infrastructure Act of 2017** (S. 1875) would require DOE to: develop model standards for the electric distribution grid, in part to improve security with respect to physical threats (§5(d)(1)), evaluate whether new performance standards and testing procedures are needed to ensure electrical equipment resilience in the face physical threats (§5(d)(2)), and submit to Congress methods and guidelines for calculating the costs and benefits of investments in resilience and security solutions for the electric grid (§5(e)(1)).
- **House Resolution 334** states that it should be the policy of the United States to, among other things, “bolster the reliability, affordability, diversity, efficiency, security, and resiliency of domestic energy supplies, through advanced grid technologies,” and to promote advanced grid tools “to increase data security, physical security, and cybersecurity awareness and protection.”

## Policy Issues for Congress

Although NERC’s CIP-014 standards have been promulgated, and bulk power asset owners have begun enhancing physical security, Congress continues to be concerned about the current state of electric grid physical security. Among many issues of potential interest, Congress may focus on several with overarching policy significance: security implementation oversight, cost recovery, hardening vs. resilience, and the quality of threat information.

## Oversight of Physical Security Implementation

Although FERC’s statutory authority for grid reliability and NERC’s reliability standards both include provisions for oversight and enforcement, congressional oversight of physical security implementation may be a challenge for several reasons. First and foremost, information about physical security measures is inherently sensitive and there are both statutory and regulatory restrictions on its disclosure.<sup>99</sup> Therefore, the level of security-related information that utilities are willing or able to provide outside the CIP-014 third-party review process or NERC compliance audits is more limited than reports about, say, general reliability or safety.

NERC is not compiling a centralized database of critical assets or security measures implemented by the utilities subject to its physical security standard. Moreover, while NERC may provide security information to FERC, the security-related information NERC can provide in public reports is limited and typically redacted. Therefore, although information about CIP-014 implementation exists among the utilities and independent third parties (operating within the standard), and is provided at some level of specificity to NERC, that information may not be as useful or visible as it could be to Congress or other outside entities.

Another oversight challenge arises because NERC’s CIP-014 standards are not prescriptive; bulk power asset owners have considerable discretion in the nature and timing of the physical security measures they may include in their physical security plans. NERC viewed such flexibility as necessary for its standard due to the unique characteristics of each utility’s bulk power system and the risks it faces. However, this flexibility also may make it more difficult to develop useful metrics for CIP-014 implementation and comparing implementation among asset owners. NERC’s standards for power grid physical security may ensure considerable consistency in the *process* utilities must undertake to identify critical substations and develop plans to secure them. However, they may not ensure consistency among the various security plans nor in the specific measures the individual asset owners will choose to implement to reduce the risk of intentional attacks. For example, ballistic shielding at critical substations may be an appropriate and sufficient protective measure for some utility assets, say, in open and rural areas, but not necessarily in more urban areas.

Even when detailed company-specific information about physical security measures is available, it might be difficult to develop reliable metrics to evaluate it. Metrics are an important tool NERC uses to evaluate utility performance in the context of power grid reliability.<sup>100</sup> However, officials at EEI have stated that measuring the adequacy of grid security for a diverse set of asset owners under changing risk circumstances poses significant problems. “Security metrics (for both cyber and physical security) have consistently been a challenge due evolving threats and vulnerabilities. If you build an eight-foot fence, the attacker just needs to bring a nine-foot ladder.”<sup>101</sup> NERC is actively engaged in efforts to develop bulk power system security metrics in which it has likewise encountered “challenges associated with developing relevant and useful security metrics that rely on data willingly and ably provided by individual entities.”<sup>102</sup>

<sup>99</sup> FERC regulations for the submission, designation, handling, sharing, and dissemination Critical Energy/Electric Infrastructure Information (CEII) are at 18 C.F.R. § 388.113.

<sup>100</sup> See NERC, “Reliability Indicators,” web page, <http://www.nerc.com/pa/RAPA/Pages/ReliabilityIndicators.aspx>.

<sup>101</sup> Chris Hickling, Edison Electric Institute, “RE: CIP-014 Implementation Update,” email to CRS, October 30, 2017.

<sup>102</sup> NERC, *State of Reliability 2017*, June 2017 p. vii. For an expansive discussion of NERC’s efforts to develop security metrics, see Appendix G in this NERC report.



Congress may judge the effectiveness of the CIP-014 physical security standards as best it can based on reports and testimony from NERC and FERC as well as information from the assets owners themselves. However, due to the issues above, if Congress decides the information as currently structured is insufficient to draw reliable conclusions about the status of bulk power physical security as a whole, it may revisit how the responsible agencies collect, measure, and report it. Congress may also consider additional avenues for reviewing this information, for example, through classified briefings or specifically requested studies or reports. Also, as FERC continues to implement its policy of regulating physical security of the power grid, Congress may examine whether company-specific security initiatives appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid overall uniformly reflect terrorism risk from a national perspective.

## Financial Requirements and Cost Recovery

Two of the barriers to physical security investment among utilities prior to the Metcalf attack were competition for limited capital investment resources and justifying security spending to corporate boards and utility rate regulators. NERC regulatory requirements for physical security make it easier for security managers to justify related operating and capital expenditures to corporate leadership, and to seek cost recovery for such expenditures through regulated rates. However, even where regulators have been supportive of cost recovery for physical security investments in general, they have faced challenges gauging the prudence of specific security investments because they are hard to evaluate on a traditional benefit-cost basis. As a 2006 report from the Electric Power Research Institute states,

Security measures, in themselves, are cost items, with no direct monetary return. The benefits are in the avoided costs of potential attacks whose probability is generally not known. This makes cost-justification very difficult.<sup>103</sup>

Note that cost-justification requires not only the approval of utility management, but also of FERC and potentially state public utility commissions which regulate the rates grid owners may charge for electric transmission and distribution service. Regulators are responsible for ensuring that electricity rates are just and reasonable. They must be convinced that any new grid security capital costs and expenses are necessary and prudent before they will allow them to be passed through to ratepayers. However, corporate financial processes differ from utility to utility, and utility rate regulation differs from jurisdiction to jurisdiction, so investment and cost recovery for physical security is not uniform across the electricity sector and remains a work in progress. As implementation of new physical security plans under CIP-014 continues, Congress may examine whether the overall level of investment appropriately reflects the level of security risk facing the bulk power system, and whether any cost-recovery barriers are preventing assets owners from making investments necessary to secure the grid.

## Hardening vs. Resilience

There are two fundamental approaches to reducing the risk of a successful physical attack on the electric grid. The first approach, which is the principal approach of NERC's CIP-014 standards, is to prevent attacks by monitoring critical facilities to identify would-be attackers before they attempt an attack, preventing attacker access to critical assets, and otherwise hardening facilities

<sup>103</sup> Electric Power Research Institute (EPRI), *Technologies for Remote Monitoring of Substation Assets: Physical Security*, March 2006, p. viii.

to make them more physically secure to protect against attack and equipment failure. The second approach is to make the broader power system more “resilient” to a successful attack on particular assets through an enhanced ability to manage loads, reroute power flows, and access other sources of generation to reduce the potential of blackouts even if critical assets are disabled.<sup>104</sup> Initiatives such as the spare transformer program administered by the Edison Electric Institute (EEI, the electric utility trade association), and a proposed federal Strategic Transformer Reserve, which can accelerate replacement of critical transformers if they are damaged, may contribute to the power grid’s ability to sustain a terrorist attack without widespread grid failure.<sup>105</sup> Thus, while hardening is aimed more at reducing the likelihood of a successful attack, resilience aims at reducing potential consequence; doing either reduces overall security risk.

Measures to harden critical facilities and measures to increase system resilience are not exclusive of one another. In fact, they can be complementary in reducing overall security risk. However, they may involve different approaches to power grid operation and design, and they may involve different, competing types of investment (e.g., transformer shielding vs. transmission network sensors). Balancing the two approaches to most efficiently achieve a desired level of physical security is a challenge for utilities with limited capital budgets. The CPUC stated that “determining appropriate security measures or approaches to ensuring resiliency” was one of three “major issues” in its power grid physical security proceedings.<sup>106</sup> As Congress continues its oversight of bulk power physical security regulation, it may consider whether the electric power sector as a whole is striking an appropriate balance between these two approaches.

## Threat Information

The utility industry’s physical security risk assessments rely upon threat information from the federal government, among other sources.<sup>107</sup> The quality of this threat information is a key determinant of what bulk power asset owners need to be protecting against and what security measures to take. Incomplete or ambiguous threat information may lead to inconsistency in physical security among grid owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat.

As discussed earlier in this report, the E-ISAC plays a valuable role in identifying and analyzing physical security risk, and disseminating information about those risks to bulk power asset owners. Independent third-party verification of risk assessments under the CIP-014 standards, together with NERC compliance audits, are two additional means of helping to ensure greater consistency of threat information among utilities. Nonetheless, a changing threat environment continues to pose challenges for physical security planning and investment. As NERC stated in a

<sup>104</sup> For a discussion about power grid resiliency and associated federal efforts, see *Government Accountability Office, Electricity: Federal Efforts to Enhance Grid Resilience*, GAO-17-153, January 2017.

<sup>105</sup> For details about electric sector spare transformer programs, see Department of Energy, *Strategic Transformer Reserve*, report to Congress, March 2017.

<sup>106</sup> CPUC, January 2018, p. 5.

<sup>107</sup> Much of this information is communicated primarily through the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the sector’s communications channel for security-related information, situational awareness, incident management, and coordination. The ES-ISAC was established under Presidential Decision Directive 63, May 22, 1998. The ES-ISAC is operated by NERC in collaboration with the DOE and Electricity Subsector Coordinating Council. Members may anonymously share information by means of a secure Internet portal. Registered users receive information on security threats and alerts, remediation, task forces, events, and other security-specific resources.

recent compliance report, “the security threat landscape is constantly changing and requires adaptation and information sharing on how best to address these issues in an effective and efficient manner.”<sup>108</sup>

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.<sup>109</sup> Threat information continues to be an uncertainty in the case of power grid physical security. For example, although there is wide consensus that the Metcalf attack was extremely alarming, some industry analysts have opined that FERC’s physical security order nonetheless may have been an “overreaction” to Metcalf.<sup>110</sup> By contrast, former DHS Secretary Michael Chertoff has predicted that “the sophistication and resulting damage of the Metcalf attack will ... be exceeded” in a future attack.<sup>111</sup> Still others have expressed concern that FERC’s physical security concerns may be too heavily focused on another Metcalf-type scenario—the last threat—rather than a wider range of potential future threats.

As discussed earlier, there is widespread belief that bulk power critical assets are vulnerable to physical attack, that such an attack potentially could have catastrophic consequences, and that the risks of such attacks are growing. But the exact nature of such potential attacks and the capability of perpetrators to successfully execute them are uncertain. Consequently, despite the technical arguments, with limited information about potential targets and attacker capabilities, the true vulnerability of the grid remains an open—and evolving—question. As Congress seeks to establish the best policies to address bulk power physical security, it may examine how federal and electric sector threat information is developed and used by critical asset owners, and how limitations and uncertainty of this information may affect physical security of the electric grid.

## Conclusion

The 2013 attack on the Metcalf transformer substation marked a turning point for the U.S. electric power sector. The attack prompted utilities across the country to reevaluate and restructure their physical security programs. It also set in motion proceedings in Congress and at FERC which resulted in the promulgation of NERC’s CIP-014 mandatory physical security standards in 2015. Based on discussions with FERC and NERC staff about utility compliance, as well as a review of public information about the activities of bulk power asset owners (and the vendors supplying them), there appear to be physical security improvements underway among owners of bulk power critical assets. The public record is too anecdotal to assert conclusively that these changes are occurring uniformly and at every relevant utility, but NERC’s summary compliance reports so far have been positive, especially for such a new standard. As NERC concluded in its *State of Reliability 2017* report,

What NERC can measure is that no major cyber- and few physical-related load losses have happened to date; that extremely low numbers of incidents have occurred on the

<sup>108</sup> NERC, *Compliance Monitoring and Enforcement Program Quarterly Report, Q3 2017*, November 8, 2017, p. 8.

<sup>109</sup> See, for example, Philip Shenon, “Threats and Responses: Domestic Security,” *New York Times*, June 5, 2003, p. A15.

<sup>110</sup> Deborah Carpentier, “NERC Gains in Vegetation Management, Cyber and Physical Security, and Reliability Assurance,” *Natural Gas & Electricity* (Wiley Periodicals), May 2014, p. 31, <http://www.crowell.com/files/NERC-Gains-in-Vegetation-Management-Cyber-and-Physical-Security-and-Reliability-Assurance.pdf>.

<sup>111</sup> Michael Chertoff, “Building a Resilient Power Grid,” *Electric Perspectives*, May/June 2014, p. 35.

operating side, and that attention to security performance has been excellent on the corporate side.<sup>112</sup>

Although the electric power sector seems to be moving in the direction of more extensive physical security, many measures have yet to be implemented and the process of corporate realignment around physical security is still underway. As the CPUC has stated,

It appears that the North American electric industry is in intermediate stages of fully harnessing the potential of security technologies and staff expertise, and integrating security and risk assessment values into the utility culture such that utility physical security ultimately is prioritized on par with safety and reliability.<sup>113</sup>

Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector's own assessments of risk. Bulk power physical security remains a work in progress. As CIP-014 implementation and other physical security initiatives proceed, Congress may seek to maintain its focus on the power sector's overall progress, not only on short term compliance with NERC's security standards, but also on structural changes supporting physical security as a priority far into the future.

## **Author Contact Information**

Paul W. Parfomak  
Specialist in Energy and Infrastructure Policy  
pparfomak@crs.loc.gov, 7-0030

---

<sup>112</sup> NERC, June 2017, p. 59.

<sup>113</sup> CPUC, January 2018, p. 57.

From: (b) (6)  
 To: Andrew Dodge; (b) (6)  
 Cc: Harry Tom  
 Subject: Did gunman open fire on Lake Worth transformer, blacking out city?  
 Date: Friday, September 14, 2018 7:01:15 AM

---

(b) (5)

---

(b) (5)

---

(b) (5)

## Did gunman open fire on Lake Worth transformer, blacking out city?

By [Joe Capozzi](#) - Palm Beach Post Staff Writer

---

LAKE WORTH —

It was disturbing enough that a transformer in the city's main electrical substation exploded in a fireball on a calm April night, [knocking out power](#) for seven hours to all of Lake Worth.

But after the fire was out, crews inspecting the damaged device saw something sinister — a jagged hole that looked like it was intentionally made by a projectile, perhaps even a bullet. They also noticed holes and nicks in other nearby equipment.

Did a gunman try to sabotage the city's electrical grid? Could the outage have been domestic terrorism?

Or was the culprit something all too familiar to long-term residents — faulty equipment?

Knowing that gunmen had attacked electrical equipment in California and Arkansas in recent years, city utility officials said the unusual circumstances around the explosion gave them no choice but to consider foul play.

"I don't want people to think that somebody is out there attacking us," said Ed Liberty, the city's director of electric utility. "But we have to be open to the evidence and not rule it out because we have this obligation to try to understand, as best as possible, what happened."

The FBI was called. The Palm Beach County Sheriff's Office opened an investigation. The damaged transformer was sent to a forensic lab for analysis.

Then, it happened again.

On the night of June 20, another fireball lit the sky over the same substation: A second transformer had catastrophically failed, causing a [citywide power outage](#) for nearly seven hours.

No suspicious holes were found on the second damaged device, which was directly next to the one that failed April 9. But that offered city officials little comfort.

More than two months later, they still don't know why two transformers, which both passed technical tests when they were installed next to each other in March, failed without warning within a span of nearly three months.

Although PBSO investigators don't suspect foul play, city officials say they can't rule out an intentional act until the forensic investigations of both damaged transformers are completed later this year.

"There's too much evidence leaning both ways," said Walt Gill, assistant director. "Until the



final report comes out, I'm not going to hang my hat either way."

## 'They are sitting ducks'

If it was foul play, it wouldn't have been the first time someone intentionally tampered with the city's electric utility.

Last year, someone with an imaginative mind hacked into a database of pre-written public alerts, which are automatically posted online when the power goes out. During Hurricane Irma, an alert blaming an outage on "extreme zombie activity" was caught by city officials before it posted online.

But eight months later, the same zombie alert somehow made it online long enough during a 30-minute outage in May for residents to see it. It went viral, resulting in international headlines and lots of laughs.

The city still doesn't know who was responsible, but the zombie alerts seemed like a fitting metaphor for the utility's troubled past. For decades, Lake Worth has struggled with problems on its power grid — from sporadic outages to aging equipment, all generating sharp criticism from residents fed up with high rates and spotty service.

Utility officials say they are making strides to improve service. But because of that troubled history, they can understand if some longtime residents might have been skeptical when [sabotage was first mentioned](#) at a public meeting in July as a possible cause of the April 9 outage.

But the other troubling reality is that attacks on power stations in North America are not unheard of. Many are the result of vandals making mischief or bored hunters taking pot shots at tantalizing targets on utility poles, incidents that rarely make headlines.

Others, though, have been more serious.

In April 2013, a gunman with a precision assault rifle fired [more than 100 shots](#) at an [electrical substation in San Jose](#), Calif., causing millions of dollars in damage to 17 giant transformers that feed power to Silicon Valley. Officials at Pacific Gas & Electric avoided a blackout by rerouting power around its Metcalf substation, but it took 27 days to bring the station back to life. No arrests were made.

Although the FBI ruled out terrorism, Jon Wellinghoff, who was chairman of the Federal Energy Regulatory Commission at the time, disagreed and called the Metcalf attack "the most significant incident of [domestic terrorism](#) involving the grid that has ever occurred."

That same year, transformers and power stations in rural [Arkansas were targeted](#) in three consecutive attacks that led to the arrest of [a local man](#) who the FBI said acted alone. And in October 2013, members of a drug cartel used guns and Molotov cocktails to attack 18 power stations in Mexico, knocking out power for 420,000 people for 15 hours.

Those attacks highlighted what utility executives and federal energy officials have worried about for years — that the [electric grid is vulnerable to sabotage](#), said Tom Carlton of Illinois-based Infrastructure Defense Technologies.

From large transmission towers to power lines attached to poles, most electrical equipment sits out in the open, often in remote locations, protected only by chain-link fences.

"They are what we in the homeland security defense business call 'soft targets' because they are unprotected by security personnel," said Carlton, whose firm specializes in perimeter security.

“They are sitting ducks, every one of them, for the most part.”

## **Installed in March**

The two transformers that exploded at Lake Worth’s Hypoluxo substation were inside a large rectangular area surrounded on three sides by 20-foot cinder-block walls and on the north side by a 6-foot chain-link fence topped with barbed wire.

The substation is often referred to as the city’s “tie-in line” because it’s the only location where city power lines tie in with the Florida Power & Light transmission system that winds throughout the state like an interstate highway network. It functions as an off-ramp from FPL’s main lines, distributing 138,000 volts through a local network of transformers to the city’s main plant and, ultimately, to 27,000 customers in the city.

The transformers that exploded in April and June are connected to the substation, but they are used only to measure the amount of electricity, or electrical current, coming in from FPL. Technically called “current transformers,” they’re casually referred to in the industry as CTs.

Each is about 8 feet high with a skinny ribbed porcelain body topped by a square tank covered by a protective weather dome, bearing an abstract resemblance to a robot.

The ones that exploded were made in 1995 by GEC Alsthom. They had been used for years at other locations in the city without incident before being moved into storage, Liberty said. He did not know when or why they were taken out of service.

They were re-installed at the Hypoluxo substation in March along with a third CT, each mounted next to the other atop 10-foot-high steel pedestals.

All three passed mandatory technical tests before they were put back into service, said Liberty. And the two that experienced sudden catastrophic failures showed no signs of an impending problem, he said.

## **Did someone fire a shot?**

At 11:14 p.m. on April 9, one of the three CTs exploded, plunging the city into darkness. Minutes later, utility crews from the city and FPL arrived at the Hypoluxo substation and saw flames leaping from the top of the transformer.

When the device cooled down to allow a safe inspection, a crew member in a lift bucket discovered a large hole on the side of the protective dome atop the transformer. The hole faced north toward a tree line visible through the chain-link fence.

“Inside that bowl you see this thing that looks like a softball-size chunk and that lined up with the hole on the side,” Liberty said. “It looked like somebody took a shot at it. It looked like a projectile had gone through it.”

They also noticed two small dents on a copper pipe, 25 feet above the ground, that supplied power to the transformer. And on the chain-link fence, they saw bullet holes on metal informational signs, holes that lined up with the damaged transformer.

“Your first reaction is to look around and make sure no one out there is aiming a gun at you. You’re hoping whoever did it is not around,” recalled Michael Jenkins, the city’s energy delivery manager, describing the reaction of many of the 20 utility crewmen on site that night when gunman suspicions were first raised.

The next day, Jason Bailey, senior system operator for Lake Worth, called the sheriff’s office and reported that the transformer looked like it “had been tampered with.” Deputies notified

the FBI, following protocol with suspicious incidents to public utility equipment, but the agency held off on getting involved and told PBSO to investigate, Liberty said.

The large hole on the side of the transformer's dome "raised the suspicion that the transformer may have been purposely targeted and shot at with an unknown firearm," according to [a PBSO report](#).

On April 12, detectives inspected the substation. From the ground, they noted that the dents on the copper pipe "appear to have similar indentations consistent with a metal projectile striking another metal object." Citing danger from the high voltage lines, deputies said they could not look closer to confirm whether or not the dents were made by bullets.

Deputies canvassed the substation and the surrounding field for shell casings but couldn't find any. They also spoke to the residents of three nearby homes. None reported hearing gunshots, but they did recall hearing "a loud boom" and seeing the transformer on fire.

A search for shell casings in the neighborhood came up empty. And PBSO records showed no calls about gunfire in the area that week.

## No evidence of a crime

Deputies also went to the city's utility yard on Second Avenue North, where the damaged transformer had been taken earlier that day. They found no indications of damage from an outside projectile. The edges of the hole in the protective dome were "peeled outwards indicating an extreme pressure build up internally from an explosion," the report said, contradicting the initial assessment by utility workers.

"On one side of the housing there is a large hole not consistent with an impact from a bullet. I could not find any fragments inside the housing, which would be components of a bullet such as copper jacketing or pieces of a lead core," an investigator wrote.

Liberty said he doesn't dispute PBSO's report, but he said he and other utility officials thought parts of the hole looked like they peeled inward.

Bailey told deputies he still thought the damage to the CT "appeared suspicious." He explained that when a transformer fails, monitors at the utility's operations center would have shown a steady drop in power prior to the failure. In this case, he said, the power flow had been normal until the moment the device exploded.

The report makes no mention of the bullet holes on the metal information signs attached to the chain-link fence, but Liberty concedes that those holes might've been there before the CT failed.

PBSO filed the case as "an information report until further evidence is presented that a crime was committed."

The city sent the damaged transformer to a lab at George Tech University, called the National Electric Energy Testing, Research and Applications Center, for forensic analyses.

The final report, which will cost the city at least \$18,000, is expected later this year. But a preliminary draft doesn't mention an outside projectile as a cause and instead points to an internal failure with the device.

Oil samples from the transformer, taken by the city, showed moisture that had somehow breached the device. That moisture may have caused insulation material inside the CT to deteriorate, generating combustible gases, according to a draft summary of the preliminary report.

But city officials say there's no way to know when or how the moisture got into the oil. It could have come from rain that fell on the damaged CT after the explosion but before the transformer was removed from its pedestal. And while the moisture might have gotten in before the explosion, as the NEETRAC draft summary indicates, city officials say they saw no signs of leakage on the device when it was tested and installed.

Before NEETRAC finished its preliminary report on the April 9 incident, the second transformer exploded. City officials saw no suspicious marks on that device, but they are sending it to Georgia Tech for analysis, too. That second CT also had signs of moisture breach, according to oil samples taken by the city.

The city's third CT was taken off line as a precaution. The city has ordered four new ones at a cost of \$50,000. Until they are installed later this year, FPL has agreed to temporarily take over the role of measuring the amount of current the city takes from the substation, Liberty said.

Later this year, the city will replace the chain-link fence on the north side of the substation with another concrete block wall, meaning the entire substation will be protected in a roofless tomb 20-feet high.

City officials hope the final report rules out sabotage, which the preliminary report did not do.

"You're trying to walk a fine line and not panic the population," Liberty said. "But no data told us ahead of time that the device was about to fail and suddenly it fails. And we have evidence suggesting an outside cause.

"We don't know what it is, but it's certainly not something that should have happened."

(b) (6)

Electrical Engineer

Federal Energy Regulatory Commission

Office of Energy Infrastructure Security (OEIS)

888 First Street, 91-60

Washington, DC 20426

Phone – 202-502-8472

(b) (6)

*Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed and should not be copied or forwarded to others without the permission of the sender. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and not necessarily those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.*

**From:** (b) (6)  
**To:** (b) (6)  
**Subject:** FW: Resilience Report  
**Date:** Monday, March 26, 2018 1:17:47 PM  
**Attachments:** [NAP resilience summary.docx](#)  
[Enhancing the Resilience of the Nations Electricity System.pdf](#)

---

FYI

---

**From:** (b) (6)  
**Sent:** Thursday, March 22, 2018 10:35 AM  
**To:** Harry Tom <harry.tom@ferc.gov>; (b) (6) David Andrejcak  
<david.andrejcak@ferc.gov>  
**Cc:** Andrew Dodge <Andrew.Dodge@ferc.gov>  
**Subject:** Resilience Report

Harry, (b) (6), and Dave,

Attached is a requested draft summary of the National Academies report on Resilience. I've added Dave A to this distribution and cc'd Andy for his information.

I've attached a PDF of the report. I have Joe's hard copy – I can return it via (b) (6)

(b) (6)  
Federal Energy Regulatory Commission  
Office of Energy Infrastructure Security  
(b) (6)



# RESILIENCE FOR **GRID SECURITY** EMERGENCIES

**Opportunities for Industry–Government Collaboration**

**National Security Perspective**



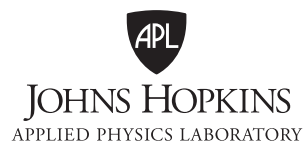
Paul N. Stockton



# **RESILIENCE FOR GRID SECURITY EMERGENCIES**

Opportunities for Industry–Government Collaboration

Paul N. Stockton



Copyright © 2018 The Johns Hopkins University Applied Physics Laboratory LLC. All Rights Reserved.

This National Security Perspective contains the best opinion of the author at time of issue. The views expressed in this study are solely those of the author and do not necessarily reflect the opinions, practices, policies, procedures, or recommendations of the US Department of Energy or any other US government agency or of JHU/APL sponsors.

## Contents

Figures.....	v
Summary .....	vii
<b>Developing Emergency Orders under the FPA.....</b>	<b>1</b>
Drafting Template Emergency Orders before Attacks Occur .....	3
Participants in Drafting and Implementing Emergency Orders .....	5
Goals and Specific Design Requirements for Developing Emergency Orders .....	11
<b>Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies .....</b>	<b>13</b>
Threats That Can Trigger Grid Security Emergencies .....	13
Thresholds for Declaring Grid Security Emergencies .....	17
Data Sharing and Consultations with Industry .....	25
<b>Grid Security Emergency Phases and Order Design Options .....</b>	<b>28</b>
Preattack Options.....	29
Extraordinary Measures when Attacks Are Occurring.....	33
Emergency Orders to Support Power Restoration.....	35
<b>Additional Emergency Order Design Parameters and Supporting Initiatives .....</b>	<b>38</b>
Deterring and Defeating US Adversaries.....	38
Communications Requirements for Issuing and Employing Emergency Orders .....	46
The Deeper Value Proposition for Emergency Orders.....	52
<b>Conclusions and Recommendations for Broader Progress .....</b>	<b>58</b>
Employing Additional Emergency Authorities for Cross-Sector Resilience.....	59
Extended Partnership Requirements within the United States and Abroad.....	64
Playing Defense in Cyberwarfare .....	70
Bibliography .....	75
Acknowledgments.....	93
About the Author .....	93





Figures

Figure S-1. Grid Security Emergency Phases..... viii

Figure 1. Stakeholders for Building Grid Security Emergency Resilience..... 10

Figure 2. ODNI Cyber Threat Framework..... 20

Figure 3. Elements of the Cyber Incident Severity Schema ..... 21

Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies..... 26

Figure 5. Emergency Order Matrix: Examples of Order Designs ..... 29

Figure 6. Categories for Protecting Defense Critical Electric Infrastructure ..... 41

Figure 7. NERC Regional Entities across North America ..... 67

Figure credits:

Figure 2: “The Cyber Threat Framework,” ODNI (Office of the Director of National Intelligence), n.d., <https://www.dni.gov/index.php/cyber-threat-framework>.

Figure 3: DHS (US Department of Homeland Security), *National Cyber Incident Response Plan* (Washington, DC: DHS, December 2016).

Figure 7: Information from NERC (North American Electric Reliability Corporation), <http://www.nerc.com/Pages/default.aspx>; figure reprinted from Susan Lee, Michael Moskowitz, and Jane Pinelis, *Quantifying Improbability: An Analysis of the Lloyd’s of London Business Blackout Cyber Attack Scenario*, National Security Report NSAD-R-18-027 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018).



## Summary

The US Congress has opened the door to novel strategies for defending the country's electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act (FPA) in December 2015, Congress granted the secretary of energy vast new authorities to use when the president declares a grid security emergency. Most important, the secretary can issue emergency orders to power companies to protect and restore grid reliability when attacks on their systems are "imminent" or under way.<sup>1</sup> The FPA is silent, however, on what the secretary might require companies to do and how such orders can bolster their emergency operations.

The onset of an attack would be the worst possible time to develop emergency orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid. They could then adjust such orders to fit the specific circumstances of an attack. Developing emergency orders in advance would also help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. Companies could then exercise their contingency plans to build preparedness for response operations and contribute to national security in unprecedented ways.

This report is structured to help the electricity subsector and Department of Energy (DOE) develop emergency orders to defend the grid against potentially catastrophic cyber and physical attacks. The report highlights the phases that grid security emergencies are likely to entail. It analyzes the requirements that emergency orders will need to meet for each phase, and how orders can supplement existing utility plans and capabilities to fill gaps in grid resilience. The report also examines how emergency orders can strengthen deterrence against grid attacks and help defeat adversaries if deterrence fails.

The president must declare a grid security emergency before the secretary of energy can issue emergency orders. However, the FPA offers only broad and potentially ambiguous criteria for making that determination, especially for attacks that are imminent. Such ambiguity is useful; the president should retain the flexibility to declare grid security emergencies in a wide range of circumstances. Nevertheless, policy makers may find it useful to establish more detailed criteria to support their internal deliberations. This report proposes options for them to consider, including criteria derived from the electric industry's requirements to preserve "adequate levels of reliability" against cascading blackouts and other multistate grid disruptions. The report also examines how industry and government agencies can refine their information sharing mechanisms to support the emergency declaration process.

Once the president makes such a declaration, grid security emergencies may roll out in three phases, each of which provides the basis for developing a distinct set of template emergency orders. Figure S-1 illustrates these phases. The first will occur if the president determines that an attack is imminent. A well-established basis already exists for developing preattack emergency orders. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions. Such operations might include staffing up emergency operations centers, prepositioning recovery personnel and supplies, increasing available generation to help manage grid instabilities, and taking other precautionary measures. A key advantage of many of these options is that utilities can carry them

---

<sup>1</sup> Fixing America's Surface Transportation Act, Public Law 114-94.

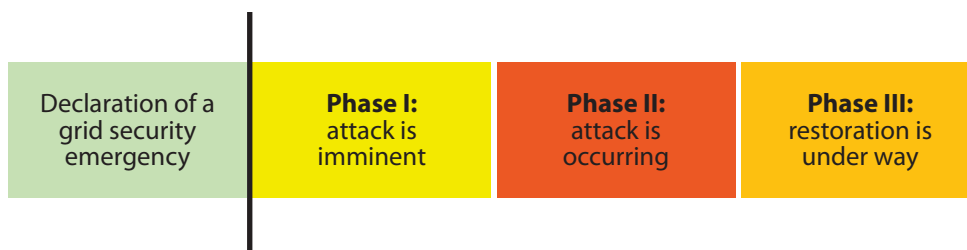


Figure S-1. Grid Security Emergency Phases

out without disrupting normal service; if the hurricane veers back to sea, utilities will have no regrets about having implemented them.

Power companies should help DOE develop equivalent “no-regrets” conservative operations to protect the grid against imminent cyber and physical attacks. A growing number of utilities are already adapting their existing plans for conservative operations to counter physical and cyber risks. These initiatives provide a strong foundation for developing emergency orders that will leverage best practices and help ensure that utilities will implement them on a consistent, nationwide basis. Moreover, because many of these conservative operations will inflict little or no disruption on normal grid service, they are ideal for protecting the grid when attacks are increasingly probable but not certain to occur. DOE and industry should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The next phase of grid security emergencies will occur when attacks are under way. Emergency orders for this phase can help utilities prevent power failures from cascading across the United States and prioritize the sustainment of electric service for military bases and facilities essential for public health (e.g., major regional hospitals and metropolitan water systems). As with conservative operations, existing electric industry plans and capabilities provide a strong basis for developing such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Orders for equivalent *extraordinary measures* could provide useful arrows in the quiver in grid security emergencies.

The final phase of grid security emergencies will commence as utilities begin restoring service to areas without power. Attacks that damage or destroy large numbers of high-voltage transformers and other difficult-to-replace grid components could create outages that darken major portions of the United States for many weeks, or even months. Power companies and DOE already have initiatives under way to meet this challenge. They should also collaborate to develop emergency orders to *support restoration*, which could facilitate the movement of replacement transformers and assist utilities in other strategically vital ways.

These grid security emergency phases could overlap. In particular, once power companies begin restoring power, adversaries may launch follow-on attacks that necessitate continued load shedding and other extraordinary measures to protect grid reliability. At the outset of an emergency, utilities should prepare to receive and implement orders across all emergency phases in an integrated way.

DOE and its industry partners should also design emergency orders to fill underlying gaps in preparedness for cyber and physical attacks. Power companies already have extensive plans and capabilities to protect and restore grid reliability against these threats, in part because mandatory reliability standards require them to do so. Grid owners and operators are also spring-loaded to employ emergency measures the moment they are



needed. Indeed, the North American Reliability Corporation can fine most major US power companies if they fail to implement emergency actions to protect grid reliability.<sup>2</sup> This robust industry preparedness begs the question: what added value can DOE emergency orders provide?

The most obvious benefit lies in the FPA's provisions for regulatory waivers and cost recovery. When grid owners and operators carry out emergency orders, they may have to violate environmental standards and other regulatory requirements. The FPA now protects entities from being punished for such violations if they occur while complying with emergency orders. The act also provides for the recovery of costs that companies will incur in implementing emergency orders. This report examines how further waiver and cost-recovery measures could reinforce preparedness for grid security emergencies.

Emergency orders can also help support national security in new and far-reaching ways. Russia, China, and other potential adversaries will not strike the grid simply to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to US defense installations responsible for deploying forces to the region, as well as to ports and other civilian infrastructure that supports force projection. Emergency orders can be designed to help deter—and, if necessary, defeat—such attacks. This report proposes specific options to do so, in support of the *National Security Strategy of the United States of America* and other sources of US policy guidance.

Some of these options will require harsh and politically contentious decisions on allocating power if adversaries severely disrupt the grid. Emergency orders for prioritized load shedding provide a case in point. To help deter attacks, grid owners and operators need the ability to sustain service to critical defense installations, including those responsible for conducting response operations against (and imposing costs on) potential attackers for however long a conflict may last. The ability to protect power flows to hospitals and other facilities vital for public health and safety will be valuable as well. However, if adversaries disrupt sufficient grid generation and transmission assets, sustaining reliable service to these installations may require utilities to curtail service to other customers. Government officials—and, ultimately, the president—should make such decisions and provide political top cover and liability protections for power companies that implement them.

Grid security emergencies will also create unprecedented challenges for government and industry to communicate with the American people. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Against a backdrop of fear and uncertainty, adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks. Adversaries may also disrupt the phone and internet-based communications systems utilities typically use to coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications playbooks to prepare for grid security emergencies, and they should make doing so a core component of the emergency order development process.

DOE and its industry and government partners will need to conduct intensive follow-on work to finalize the development of emergency orders and build utility-specific contingency plans to implement the orders in ways that account for accelerating structural changes in the electricity subsector. Their collaborative efforts will

---

<sup>2</sup> Bulk power system entities, including generation and high-voltage transmission companies, are subject to NERC's mandatory reliability standards and emergency orders under the FPA. For an analysis of applicability issues, see pages 5–10.

require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, as utilities and DOE tackle the immediate challenges of developing emergency orders, they should also explore broader opportunities to build preparedness for grid security emergencies. One such opportunity lies in integrating the use of emergency orders with other federal authorities. The secretary of energy can issue grid security emergency orders only to power companies. Increasingly, however, power generation depends on the flow of natural gas. Communications systems and other infrastructure sectors will also play critical roles in supporting power restoration. The secretary of energy and other federal leaders have additional authorities beyond section 215A of the FPA that can strengthen cross-sector resilience for grid security emergencies. However, achieving these benefits will require private and public sector leaders to preplan and exercise the coordinated use of these authorities, and to develop “whole-of-government” strategies to support infrastructure owners and operators.

Coordination with Canada could be valuable as well. The electric grids of the United States and Canada are deeply interconnected, and adversary-induced failures in one nation may rapidly cascade into the other. The secretary of energy does not have the authority to issue emergency orders to power companies in Canada (or in any other nation). Yet, significant opportunities exist to build on current reliability protections and emergency coordination mechanisms between US and Canadian utilities. The United States could also develop collaborative plans with Mexico as well as US allies in Europe and Asia.

In addition, DOE and its partners should explore further opportunities to help deter cyber attacks and defeat US adversaries if deterrence fails. The US *National Security Strategy* emphasizes that the United States needs to convince adversaries not only that they will suffer costly consequences if they attack but also that attacking will not accomplish the objectives they seek—in other words, achieve deterrence by denial. Yet, leading scholars of deterrence argue that deterrence by denial will be extraordinarily difficult to establish in cyberspace. Emergency orders and implementation plans can help meet these challenges by strengthening grid resilience in novel ways. Government agencies should also consider developing broader doctrine to “play defense” if cyberwarfare breaks out, and coordinate grid security emergency operations at home with measures to suppress adversary attacks at their source.

The foundational importance of the electric grid makes it a prime target for attack. As secretary of energy Richard Perry emphasizes, “America’s greatness depends on a reliable, resilient electric grid” that can power the economy, support national defense, and provide for the necessities of modern life.<sup>1</sup> To prevent adversaries from exploiting the United States’ dependence on the grid, the Department of Energy (DOE) and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter—and, if necessary, defeat—attacks on the grid.<sup>2</sup>

The FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the Fixing America’s Surface Transportation (FAST) Act amendments to the FPA, it greatly expanded the secretary of energy’s authority to issue emergency orders to grid owners and operators. Under section 215A of the act, “the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability” of critical electric infrastructure in a grid security emergency.<sup>3</sup> Before the secretary can issue those orders, the president

must first declare a grid security emergency when attacks on the grid are imminent or under way.<sup>4</sup>

However, legislators provided scant guidance on what the secretary might order power companies to do. DOE and its partners in the electricity subsector are now assessing which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats. This report supports their work by examining possible emergency orders and analyzing broader opportunities to strengthen resilience for grid security emergencies.

## Developing Emergency Orders under the FPA: Collaborative Opportunities, Fundamental Goals, and Overarching Design Requirements

The secretary of energy’s new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, “the nine most terrifying words in the English language are ‘I’m from the government and I’m here to help.’”<sup>5</sup> Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already taking steps to minimize such risks. Especially valuable, the department has incorporated industry recommendations on the process by which the secretary should issue emergency orders to utilities, and—“if practicable”—consult with industry before those orders are issued.<sup>6</sup> The next collaborative step should be to include power companies in

<sup>1</sup> Perry, letter to the FERC.

<sup>2</sup> The 2015 FAST Act amendments to the FPA provide the authority to undertake these efforts. Prior to 2015, section 202(c) of the FPA already authorized the secretary of energy to issue emergency orders to order “temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest.” That provision also specified that the secretary could exercise such powers “during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes.” See “DOE’s Use of Federal Power Act Emergency Authority,” DOE. The 2015 FAST Act amendments to the FPA gave the secretary further powers (mostly incorporated in section 215A of the act), which are the primary focus of this report.

<sup>3</sup> 16 U.S.C. § 824o, (b)(1).

<sup>4</sup> The analysis that follows examines the definition of such emergencies in the FPA and potential thresholds for declaring them.

<sup>5</sup> Reagan, “President’s News Conference.”

<sup>6</sup> DOE, “RIN 1901–AB40,” 1176; EEI, “Comments”; and Paradise et al., “ISO-RTO Council Comments.”

designing template emergency orders. Grid owners and operators have unequaled knowledge of their own infrastructure and operating procedures and extensive experience in employing emergency measures to protect and restore grid reliability.<sup>7</sup> They are well positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses—and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders would be most useful to help defend their systems and effectively supplement the emergency measures utilities would already be taking on their own. Utilities will also play a critical role in building company-specific plans to implement emergency orders, exercising those plans, and identifying remaining gaps to fill.

Strategic guidance from DOE and other government departments will be just as critical for designing emergency orders. Federal leadership will be essential to ensure that emergency orders help achieve overarching US security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing emergency orders to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.<sup>8</sup> Government officials can also shape emergency orders and supporting initiatives to help implement US cyber resilience strategies, including the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

(May 2017) and DOE's *Multiyear Plan for Energy Sector Cybersecurity* (March 2018).<sup>9</sup>

In addition, DOE will play a critical role in coordinating industry and government operations during grid security emergencies. The same congressional amendments that granted the secretary expansive new emergency authorities also specified that DOE shall be the federal government's "lead sector-specific agency for cybersecurity for the energy sector." As such, the secretary is responsible for collaborating with grid owners and operators, regulators, and other government agencies to help mitigate incidents and provide broader support to the energy sector.<sup>10</sup>

Federal incident response operational plans provide a broader framework for building these collaborative mechanisms. Presidential Policy Directive 41, *United States Cyber Incident Coordination* (July 2016), the *National Cyber Incident Response Plan* (December 2016), and the *National Response Framework* (June 2016) offer particularly useful guidance for building grid-specific coordination mechanisms.<sup>11</sup> DOE is also strengthening its own internal mechanisms and organizational structure to manage cyber incidents.<sup>12</sup> These changes further position the department to effectively collaborate with industry in developing and executing emergency orders.

<sup>9</sup> Trump, *Executive Order on Strengthening Cybersecurity*; and DOE, *Multiyear Plan*. See also Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*; and DHS, *Cybersecurity Strategy*.

<sup>10</sup> Fixing America's Surface Transportation Act, Public Law 114-94, 1779 (hereafter cited as FAST Act).

<sup>11</sup> Obama, *United States Cyber Incident Coordination*; DHS, *National Cyber Incident Response Plan*; and DHS, *National Response Framework*.

<sup>12</sup> DOE, *Multiyear Plan*, 28. DOE has also established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to "enable more coordinated preparedness and response to natural and man-made threats." See "Secretary of Energy Forms New Office," DOE.

<sup>7</sup> FERC and NERC, *Restoration and Recovery Plans*; FERC and NERC, *Planning Restoration Absent SCADA or EMS (PRASE)*; and FERC and NERC, *Recommended Study: Blackstart Resources Availability (BRAv)*. Additional BPS plans, exercises, and mandatory reliability standards are addressed in subsequent portions of the report.

<sup>8</sup> White House, *National Security Strategy*.



## Drafting Template Emergency Orders before Attacks Occur

The FPA specifies that before issuing emergency orders “the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action,” consult with appropriate power companies and other grid resilience stakeholders.<sup>13</sup> But opportunities for such consultations may be sharply limited. Adversaries may strike the grid with little or no warning. Moreover, when attacks are imminent or under way, rapidly issuing emergency orders may be crucial to help prevent cascading failures and other widespread disruptions. This imperative for speed could make consultations impractical.

To enable collaboration and minimize the risk that DOE will have to create orders amid the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, assistant secretary of energy for electricity delivery and energy reliability, stated in March 2018: “In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.”<sup>14</sup> Power companies and other electricity subsector organizations have also emphasized the need for industry and the government to jointly develop orders before adversaries strike.<sup>15</sup>

Such collaborative efforts should initially focus on creating *template orders*: orders that lay out the

basic types of actions that the secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act amendments’ potential value for the secretary to issue general orders to “protect and restore the reliability of the grid.” Vague, overly broad directives cannot provide an adequate basis for utilities to develop system-specific plans to implement them. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for “maximum generation” and increased reserve margins to more aggressive, far-reaching measures.<sup>16</sup> A key objective for such development efforts: provide a menu of agreed-upon options from which the secretary can choose as circumstances require, supported as much as possible by consultations with industry.

Developing emergency orders before attacks occur can help ensure that, as a minimalist goal, such orders will “do no harm.” By participating in the order design process, power companies can shape orders to account for system-specific engineering constraints and requirements for emergency operations. This industry input will be especially important because DOE has the authority to punish utilities for failing to comply with emergency orders, even if they are poorly designed. DOE’s grid security emergency rule specifies that “in accordance with available enforcement authorities, the secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order.”<sup>17</sup> If

<sup>13</sup> This includes the North American Electric Reliability Corporation (NERC) and its Electricity Information Sharing and Analysis Center (E-ISAC). 16 U.S.C. § 824o–1. See also the notice of proposed rulemaking and request for comment (DOE, “RIN 1901–AB40”).

<sup>14</sup> Walker, *Written Testimony*.

<sup>15</sup> See Joint Commenters, “Comments; and NASEO, “Comments.”

<sup>16</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual* 13, 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help “maintain reliable operation while meeting . . . unexpected outages of existing capacity.” See “M-1 Reserve Margin,” NERC.

<sup>17</sup> DOE, “RIN 1901–AB40,” 1182.



power companies find that an order is impossible to implement or is otherwise objectionable, they can ask DOE to reconsider it.<sup>18</sup> But adjudicating individual emergency orders amid a grid security emergency could delay time-critical actions. Instead, DOE should include industry in developing emergency orders from the start and resolve utility concerns before adversaries strike.

Preplanning to coordinate industry and government emergency operations will also be valuable. Power companies are already poised to take immediate emergency actions to protect grid reliability as circumstances require, regardless of whether the secretary issues emergency orders. It will be helpful to understand in advance how DOE can best align the issuance of such orders with industry-initiated actions. Once attacks are under way, preplanning for operational coordination will become still more important, especially if adversaries continue striking the grid and its supporting communications systems after their initial salvo.

If attacks do occur, Russia, China, or other potential adversaries will use country-specific tactics, techniques, and procedures to disrupt US infrastructure. Defending against those attacks will require tactical and operational responses that are similarly tailored to specific adversaries. Over time, it may be possible to develop (and protect adversaries from accessing) emergency orders that account for these individualized defensive requirements. US leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this report examines opportunities to do so.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders

should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high-voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military bases, regional hospitals, and other critical customers that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and identify opportunities to improve order design and execution. Training programs to prepare employees to carry out utility-specific implementation plans should also get under way as soon as possible. On a larger scale, utilities will also be able to exercise the implementation of template emergency orders within the framework of the Cyber Mutual Assistance (CMA) Program. This program enables over 140 utilities in the United States and Canada to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.<sup>19</sup> Exercises can help determine how best to align the issuance and implementation of emergency orders with these growing capabilities for mutual support.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the secretary of energy has the sole authority to issue emergency orders, the secretary may request input from senior DOE staffers

<sup>18</sup> DOE, "RIN 1901-AB40," 1181-1182.

<sup>19</sup> "ESCC's Cyber Mutual Assistance Program," ESCC.

on which orders will be most useful against specific types of attacks. The secretary may also need to brief the president and the National Security Council on proposed orders and their potential benefits. By developing orders and clarifying their respective advantages before adversaries strike, DOE and industry partners can facilitate such deliberations.

Over the longer term, industry and government leaders might structure their collaboration to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public-private and interagency coordination.<sup>20</sup> Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government-industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, to develop template emergency orders and contingency plans to implement them, power companies will need to conduct extensive operational and engineering studies and use enhanced modeling to understand the potential impact of such orders. The FAST Act amendments to the FPA provide no funding for such development efforts. Moreover, DOE and power companies are only the most obvious participants in the order design process. A wide array of other grid resilience and incident management stakeholders may also need to assist that process—including critical ones not mentioned in the FPA. Determining which specific public and private sector organizations should help shape template orders constitutes a critical first step in preparing for grid security emergencies.

## Participants in Drafting and Implementing Emergency Orders: The Bulk Power System and the Broader Electricity Subsector

An initial task in developing emergency orders will be to determine which components of the electricity subsector should participate in that effort. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>21</sup> The most obvious candidates for inclusion are the power companies that are subject to emergency orders. The FAST Act amendments to the FPA specify which components fall into that category. Chief among them are “any owner, use or operator of critical electric infrastructure or of defense critical electric infrastructure within the United States.”<sup>22</sup> The FPA also includes criteria to identify this infrastructure. Critical electric infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>23</sup> Defense critical electric infrastructure consists of grid components that serve facilities “critical to the defense of the United States” and that are vulnerable to the disruption of grid-provided power.<sup>24</sup>

However, Congress also narrowed the definition of critical electric infrastructure in a significant way. The FPA states that such infrastructure only includes assets that compose the bulk power system (BPS). BPS assets are those “facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation

<sup>20</sup> Danzig, *Catastrophic Bioterrorism*, 5–7; and Blue Ribbon Study Panel, *National Blueprint*, 13, 42–44.

<sup>21</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>22</sup> 16 U.S.C. § 824o–1, (b)(4)(c).

<sup>23</sup> 16 U.S.C. § 824o–1, (a)(2).

<sup>24</sup> 16 U.S.C. § 824o–1, (a)(4).

facilities needed to maintain transmission system reliability.”<sup>25</sup> These BPS generation and transmission assets provide synchronized power within the three interconnections that serve the entire United States and parts of Mexico and Canada.<sup>26</sup>

As defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.<sup>27</sup> That limitation creates a potential problem for executing emergency orders. Local distribution systems often provide the “last mile” of connectivity between transmission systems and military bases and other critical customers. As DOE and industry create template emergency orders and execution plans, it will be essential to integrate local distribution providers into that development process.

However, before examining these distribution-level issues, it will first be helpful to clarify the components of the BPS that are explicitly subject to emergency orders under the FPA (and are therefore key partners for DOE in designing them). The FPA states that the secretary of energy may issue emergency orders to the following the BPS “entities:”<sup>28</sup>

**The Electric Reliability Organization.** After blackouts cascaded across major portions of the United States in August 2003, Congress authorized the Federal Energy Regulatory Commission (FERC) to certify an electric reliability organization to develop and enforce, subject to FERC approval, mandatory

electric reliability standards for all users, owners, and operators of the US BPS.<sup>29</sup> FERC certified the North American Electric Reliability Council (NERC) as the first-ever electric reliability organization in July 2006. Renamed the North American Electric Reliability Corporation in 2007, it has served in that role since.<sup>30</sup> NERC’s mission is to ensure the reliability and security of the BPS in North America. As such, NERC is uniquely positioned to help DOE develop emergency orders, especially for attacks that could create cascading blackouts or other multistate disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a leading role for the electricity subsector in establishing situational awareness, incident management and coordination, and communication capabilities.<sup>31</sup> E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be vital for responding to grid security emergencies.

**Regional entities responsible for enforcing reliability standards for the BPS.**<sup>32</sup> NERC has delegated certain authorities to eight regional entities to monitor and enforce compliance with reliability standards.<sup>33</sup> While regional entities play major oversight roles, they do not directly operate the physical grid and would not, on their own, be positioned to execute emergency orders. However, they could help utilities and DOE and preplan for

<sup>25</sup> 16 U.S.C. § 824o, (a)(1).

<sup>26</sup> Interconnections are defined as the “geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control.” North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See NERC, *Glossary*.

<sup>27</sup> The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify “local” distribution. See 16 U.S.C. § 824o, (a).

<sup>28</sup> 16 U.S.C. § 824o–1, (b)(4).

<sup>29</sup> Energy Policy Act of 2005, Public Law 109-58. This does not include Alaska or Hawaii.

<sup>30</sup> NERC, *History*. For more information on NERC, see “About NERC,” NERC.

<sup>31</sup> “Electricity Information Sharing and Analysis Center,” NERC.

<sup>32</sup> DOE, “RIN 1901–AB40,” 1177. See also 16 U.S.C. § 824o, (a)(7).

<sup>33</sup> “Key Players,” NERC. In July 2017, however, one regional entity announced its intention to dissolve. FERC has approved the dissolution, effective July 2018. See FERC, *Order Granting Approvals* (163 FERC ¶ 61,094).

issuing regulatory waivers to BPS grid operators as they comply with emergency orders.

**Owners, users, and operators of critical electric infrastructure or defense critical electric infrastructure within the United States.**<sup>34</sup> Companies that own and operate generation and transmission assets will be among the most likely recipients of emergency orders and should play a critical role in designing them. Reliability coordinators will be similarly important. Reliability coordinators are the entities that constitute “the highest level of authority” for the reliable operation of the bulk electric system (BES).<sup>35</sup> They are also responsible for maintaining a “wide-area view” of the BES and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, reliability coordinators will be critical for designing, receiving, and implementing emergency orders to counter attacks that individual BPS owners and operators may not have the ability to defeat. Seven regional transmission organizations and independent system operators, most of which are registered as reliability coordinators, also help operate and ensure the reliability of the BES in many regions of the United States.<sup>36</sup> Accordingly, regional

transmission organizations and independent system operators will be essential to the design and execution of emergency orders.

### **Local Distribution Providers and Other Grid Resilience Stakeholders**

The 2015 FAST Act amendments to the FPA do not explicitly address the possible roles of local distribution systems in grid security emergencies. However, local distribution infrastructure is critical for overall resilience against cyber and physical attacks. Even if emergency orders help defeat attacks on BPS assets, adversaries may still be able to achieve catastrophic effects by striking multiple local distribution systems and thereby interrupting the flow of power from transmission systems to military bases, hospitals, and other end users. Local distribution systems may also need to help implement emergency orders issued to BPS entities. For example, if the secretary orders transmission systems to protect reliability by shedding load, yet at the same time sustain the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding. Holistic preparedness for grid security emergencies therefore requires engagement with local distribution systems.

These systems will also have strong incentives to participate in the emergency order planning process. Just as BPS entities rely on local distribution utilities, these utilities rely on generation, transmission, and higher-voltage distribution entities to serve end users. Local systems will also share the commitment of BPS entities to protect and rapidly restore service to defense installations and other critical customers. By integrating local distribution utilities

<sup>34</sup> The analysis that follows later in this section examines the definition of “users” of critical electric infrastructure and defense critical electric infrastructure.

<sup>35</sup> While the BPS broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the BES is a subset of the BPS that includes, with some exclusions, all transmission and real and reactive power sources at one hundred kilovolts or higher. As with the BPS definition, the BES definition excludes local distribution providers. For these definitions, as well as the definition of reliability coordinators, see NERC, *Glossary*. Consistent with the FPA and the authorities it provides for handling grid security emergencies, this report focuses on the application of emergency orders to BPS entities specifically.

<sup>36</sup> There are ten regional transmission organizations and independent system operators under NERC’s purview, though three operate exclusively in Canada. Regional transmission organizations and independent system operators are independent membership-based nonprofit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are

operated by individual utilities or utility holding companies. See “About 60% of U.S. Electric Power Supply Managed by RTOs,” US Energy Information Administration. Six of the seven regional transmission organizations/independent system operators operating in the US are also current reliability coordinators. See “Reliability Coordinators,” NERC.



into emergency order planning, these utilities will be able to participate in shaping template orders and implementation plans to help achieve their reliability goals when adversaries strike. Moreover, to the extent that local distribution companies may be subject to emergency orders, they may also benefit from the FPA's liability protections and cost-recovery provisions for actions taken to execute those orders.

DOE and other stakeholders may determine that the FPA already gives the secretary adequate authority to issue emergency orders to local distribution companies. The act states that emergency orders may apply to "any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure" within the United States.<sup>37</sup> The act, however, does not further define owners, users, and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the act.

Regardless of whether the secretary can issue orders to local distribution utilities, BPS entities should include them in building the contingency plans to implement emergency orders. This preplanning will be essential to strengthen comprehensive, end-to-end protection of grid reliability against attacks.

Many companies that own transmission assets also own distribution infrastructure. These utilities will find it relatively easy to include distribution assets in their emergency planning. Integrated response plans will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for "vertically integrated" utilities that own and operate assets for all three functions. However, many municipally owned electric utilities and rural electric cooperatives (including those that serve critical and defense critical electric infrastructure) are not part of vertically integrated companies. In US regions where generation, transmission,

and distribution systems exist as separate entities, additional engagement initiatives will be essential to implement emergency orders and sustain power to essential facilities.

Including state regulators and other state officials in these integrative efforts could offer additional benefits. State public utility commissions have primary regulatory jurisdiction over distribution systems.<sup>38</sup> The National Association of Regulatory Utility Commissioners, which represents state regulators nationwide, has focused growing attention on the need for prudent utility investments in cyber and physical resilience.<sup>39</sup> Commissioners in New Jersey and other states are also leading regulatory initiatives to bolster cyber resilience in their respective jurisdictions.<sup>40</sup> Emergency managers and National Guard leaders in a growing number of states are also building new mechanisms to coordinate with utilities in responding to cyber attacks. Adding such additional partners to help design emergency orders and plan for their implementation would complicate an already far-reaching engagement process. Nevertheless, incorporating perspectives from state commissioners and other officials would help advance comprehensive state-level preparedness for grid security emergencies.

### **Additional Partners for Engagement**

DOE and power companies will need to collaborate with a wider array of partners to develop and execute some potentially useful emergency orders, especially to support grid restoration. The final rule

<sup>37</sup> 16 U.S.C. § 824o, (b)(4)(a).

<sup>38</sup> The US Constitution, in most cases, allows federal regulation of private economic activity only for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See Lazar, *Electricity Regulation in the US*, 15.

<sup>39</sup> See NARUC, *Cybersecurity*; and NARUC, *Resolution on Physical Security*.

<sup>40</sup> State of New Jersey Board of Public Utilities, *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196).



on *Grid Security Emergency Orders: Procedures for Issuance* (hereinafter referred to as the grid security emergency rule) notes: “Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits” to expedite the restoration of power.<sup>41</sup> This includes traditional partners such as the Department of Homeland Security (DHS) and the Department of Defense (DOD). Still broader collaboration with government and private sector partners may be valuable for implementing emergency orders to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy large power transformers at substations across the United States, and these attacks cut off power to critical military bases, the secretary might order industry to prioritize the replacement of large power transformers at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program to provide for such replacements.<sup>42</sup> New industry-led organizations such as Grid Assurance,<sup>43</sup> as well as programs such as the Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) initiative, are further expanding the industry’s capacity to replace transformers and other equipment.<sup>44</sup> These efforts will be essential for preparing for grid security emergencies, especially as industry stocks and securely stores the full range of replacement transformer types and sizes that large-scale physical attacks may require.

However, power companies do not move large power transformers by themselves. They rely on railroad companies, barges, and heavy-haul trucking companies to help do so and have established a

Transformer Transportation Working Group under the ESCC to plan and coordinate transformer movement.<sup>45</sup> Exercises in the Spare Transformer Equipment Program now involve representation from transportation stakeholders. Yet, the FPA does not give the secretary authority to issue orders to transportation companies. In anticipation of orders for replacing transformers, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Preplanning with the US Department of Transportation (DOT), the Federal Emergency Management Agency (FEMA), and state governments to get contracts, permits, and regulatory waivers to expedite transformer movement will also be useful. In addition, advance coordination with emergency managers at all levels of government would help them mitigate the effects of rotating blackouts or other extraordinary measures on public health and safety.

DOE and the electricity subsector should consider expanding the geographic scope of these discussions as well. In defining the defense critical electric infrastructure that emergency orders can protect, Congress excluded grid assets in Alaska and Hawaii.<sup>46</sup> But both states are home to vital military installations, as are a number of US territories. The secretary also lacks the authority to issue emergency orders to Canadian utilities. Yet, US and Canadian electric systems are deeply integrated, and coordinated efforts to prevent instabilities in grid security emergencies could benefit both nations. Collaborations with NATO allies and other security partners in the face of major adversarial cyber campaigns could be valuable as well. The concluding section of this report examines the potential benefits of expanding grid

<sup>41</sup> DOE, “RIN 1901–AB40,” 1177.

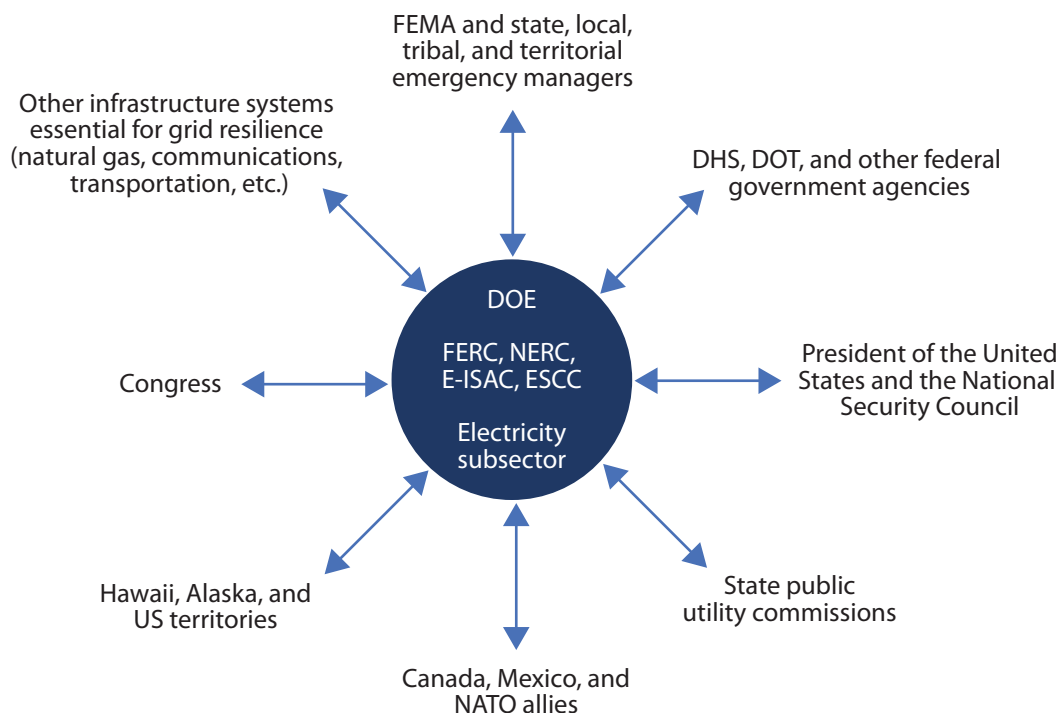
<sup>42</sup> See DOE, *Strategic Transformer Reserve*; and “Spare Transformers,” EEL.

<sup>43</sup> “Transmission Equipment Ready,” Grid Assurance.

<sup>44</sup> FERC, *Order Authorizing Acquisition and Disposition* (163 FERC ¶ 61,005), 10.

<sup>45</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>46</sup> 16 U.S.C. § 824o–1, (a)(4). The FPA’s section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).



**Figure 1. Stakeholders for Building Grid Security Emergency Resilience**

security emergency coordination within the United States and beyond.

Figure 1 illustrates the array of partners that might help build preparedness for such emergencies. DOE, BPS entities, and the broader electricity subsector comprise the core of the team needed to design, issue, and implement emergency orders. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>47</sup> This definition comprises the key subsector components represented in the ESCC, to include owners and operators of electric generation, transmission, and distribution assets “from all ownership categories.”<sup>48</sup> As such, the ESCC is ideally suited to coordinate with

DOE in the order development process, together with NERC, the E-ISAC, and other BPS entities and trade associations.

Surrounding these core participants are additional partners that might offer valuable insights for developing orders and coordinating emergency response operations. Some of these partners (including Congress) can also help oversee the implementation of the FPA’s emergency provisions and assess requirements for further statutory changes.

Of course, the full set of potential contributors to emergency preparedness is broader still. For example, vendors who can help utilities replace damaged relays and other equipment could play vital roles. So could law enforcement agencies, cybersecurity contractors, state National Guard organizations, and other sources of expertise and support for power companies. National laboratories and other research and development organizations will also need to sustain their support for improved grid resilience. Over time, comprehensive engagement with all such partners could pay major dividends.

<sup>47</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>48</sup> In addition to infrastructure owners and operators, ESCC membership includes regional transmission organizations and independent system operators, NERC, the National Infrastructure Advisory Council, and the Canadian Electricity Association. ESCC, *Electricity Sub-Sector Coordinating Council Charter*, 3.

## Goals and Specific Design Requirements for Developing Emergency Orders

The starting point in developing template emergency orders is to identify the objectives, scope, and design requirements that these orders will need to encompass. Key issues analyzed in the sections of the report that follow:

- **Threats, triggers, and thresholds for issuing emergency orders.** Only a limited number of natural and man-made hazards can trigger a grid security emergency.<sup>49</sup> Countering each of those hazards will require threat-specific emergency orders. Hence, the first step for developing such orders will be to examine the threats and attack scenarios on which the design process should focus and clarify the criteria that the president might use to determine that a grid security emergency exists—including when there is an “imminent danger” of an attack.
- **Designing emergency orders for sequential phases of grid security emergencies.** Different types of emergency orders will be needed to protect grid reliability (1) when attacks are imminent, and (2) when attacks are under way. Promising opportunities also exist to develop orders for a third phase of grid security emergency operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.
- **Incorporating national security policies and priorities into emergency order design.** Adversaries may strike the grid to disrupt the flow of power to defense installations and other facilities essential to national security. Many utilities are already collaborating with defense partners to build redundant power feeds for these facilities and make other targeted

investments in resilience. A growing number of grid owners and operators also plan to prioritize the restoration of power to military bases if blackouts occur. Emergency orders provide a unique opportunity for DOE and its partners to build on such initiatives, and provide more systematic, comprehensive, and effective support to national security.

An initial step to do so is to ensure that emergency orders reflect and help achieve broader federal government strategies to defend critical infrastructure. Most important, the US *National Security Strategy* specifies how the United States will deter attacks on critical systems and—if deterrence fails—how it will defeat the attackers.<sup>50</sup> DOE and its industry partners should design emergency orders to help implement the strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this design process with two further steps. First, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. The FPA provisions and existing industry plans to prioritize the restoration of power will provide a useful starting point. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement emergency orders and help defend the nation.

Emergency orders and implementation plans also offer a basis to clarify how US agencies and private companies will coordinate their operations during cyberwarfare, and build consensus on the private sector’s emerging role in national security. No power company has ever tried to maximize shareholder value by promising to bolster cyber deterrence or help defeat attacks by nations such as Russia or China. Yet, because

<sup>49</sup> In addition to being triggered by cyber attacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, (a)(7).

<sup>50</sup> White House, *National Security Strategy*, 13.

of the grid's importance to the economy, public health and safety, and national defense, the United States needs a doctrinal framework to coordinate industry and government actions during attacks on the US electric system.<sup>51</sup> Scott Aaronson, Edison Electric Institute's vice president for security and preparedness, notes that "there is not a lot of doctrine around cyber attacks on civilian infrastructure."<sup>52</sup> Building such doctrine and operationalizing public-private partnerships will be crucial for grid security emergency preparedness.

- **Communications.** The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The grid security emergency rule describes the consultative process that (if practicable) will occur before the secretary issues emergency orders.<sup>53</sup> However, the grid security emergency rule does not address the risk that adversaries will attack the industry-government communications systems necessary to issue orders, monitor their implementation, and defeat adversaries' attacks.

Building secure, survivable communications will be essential to effectively issuing and implementing emergency orders. However, the FPA provides no requirements or funding to do so. The electricity subsector is currently working with government agencies and telecommunications companies to advance secure communications initiatives. These partners should treat preparedness for grid security emergencies as a special area of focus, including measures to

ensure that grid owners and operators can verify the authenticity of emergency orders.

Government and utility leaders will also need to coordinate what they tell the American people when the secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including those for prioritized load shedding, could cut off electricity to many thousands of customers. Emergency orders that will have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Attackers will strike the grid to achieve political benefits, including, potentially, the incitement of public panic and a loss of confidence in US leaders. To promote unity of messaging against such efforts, it will be essential to build on existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders.

- **Waivers and cost recovery.** Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the act itself, FERC-approved reliability standards, or environmental regulations.<sup>54</sup> However, emergency orders will be easier to implement if they include preplanned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

<sup>51</sup> For DOD's definition of doctrine and an analysis of its benefits for joint warfighting, see Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United State*.

<sup>52</sup> Lynch, "How the Russian Government Allegedly Attacks."

<sup>53</sup> DOE, "RIN 1901-AB40," 1181.

<sup>54</sup> These waivers apply unless companies carry out orders and related actions in a "grossly negligent manner." See 16 U.S.C. § 824o-1, (f)(4).



The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.<sup>55</sup> Industry–government dialogue will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader preplanning needed for the financial turbulence that grid security emergencies could create. This study also examines possible emergency orders that would require investments in grid infrastructure to implement. The FPA does not authorize government spending on such pre-emergency projects. If DOE and its partners decide that investment-dependent orders have sufficient value for grid resilience, these partners (and Congress) should explore government funding options that reflect the national security benefits of such orders, rather than increase the electricity bills paid by private citizens.

- **Opportunities for broader resilience against grid security emergencies.** Power companies and DOE may find it helpful to develop a comprehensive plan to sequence and integrate all of the initiatives outlined above. Such a plan might also account for three additional opportunities for progress: (1) employing additional government authorities to coordinate emergency operations between electric utilities and companies in other infrastructure sectors, including the natural gas providers on which power generation increasingly depends; (2) deepening US partnerships with Canada to help protect the interconnected North American power grid, and exploring opportunities for collaboration with Mexico and other nations; and (3) examining longer-term opportunities to leverage improvements in grid resilience to strengthen cyber deterrence, and assessing the risks and potential benefits of coordinating cyber defense operations at home and abroad.

## Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies

The FPA leaves the president substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should build consensus on the types of threats that ought to drive and sequence the development process. These partners should also examine possible decision criteria and consultative mechanisms to support declarations of grid security emergencies.

### Threats That Can Trigger Grid Security Emergencies: Implications for Emergency Order Design

A broad array of natural and man-made hazards, including earthquakes and severe weather events such as hurricanes and ice storms, can cause multistate blackouts. However, in amending the FPA, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the “occurrence or imminent danger” of:

(A)

(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;<sup>56</sup> and

(ii) disruption of the operation of such devices or networks, with significant adverse

<sup>55</sup> 16 U.S.C. § 824o–1, (b)(6).

<sup>56</sup> The second section of this report defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of grid security emergency thresholds.



effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event;

or

(B)

(i) a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and

(ii) significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.<sup>57</sup>

Protecting critical and defense critical electric infrastructure against each of these threats will require different types of emergency orders—though some potential orders may be useful against multiple hazards. The threats will also pose disparate challenges for determining whether a grid security emergency is imminent or under way. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the president faces uncertainties about the likelihood and potential consequences of a grid security emergency.

### Geomagnetic Storms as a Possible Initial Focus

Emergency orders for geomagnetic disturbances will entail fewer design challenges than those for cyber attacks and other man-made hazards, and therefore provide opportunities for rapid progress. Geomagnetic disturbance events occur when coronal mass ejections on the sun create geomagnetically induced currents on the earth's surface. These currents can damage unprotected transformers and other grid infrastructure. Compared with the other threats that can trigger grid security emergencies, determining that there is imminent danger of a geomagnetic disturbance event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the president decide whether

to declare a grid security emergency and will provide significant warning before geomagnetically induced currents threaten to damage grid infrastructure.

Industry and government partners can develop emergency orders to take advantage of this warning time. For example, the secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of geomagnetically induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.<sup>58</sup>

A strong foundation already exists for drafting such orders. Studies of the effects of geomagnetic disturbances on the power grid have contributed to a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.<sup>59</sup> Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the federal government to ensure that it has the capability to predict and detect space weather events and the ability to communicate these assessments to public and private sector stakeholders. The order also requires the development of protection and mitigation plans for critical infrastructure and plans for response and recovery if geomagnetic disturbances occur. In addition, the order requires sector-specific agencies to “assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event.”<sup>60</sup>

NERC reliability standards provide an additional cornerstone for developing emergency orders for geomagnetic disturbances. TPL-007-1—*Transmission System Planned Performance for Geomagnetic*

<sup>58</sup> Phillips, “Solar Shield.” See also MISO, *Geomagnetic Disturbance Operations Plan*, 5.

<sup>59</sup> See “NOAA Space Weather Scales,” NOAA; and Kappenman, *Geomagnetic Storms*.

<sup>60</sup> Obama, *Executive Order—Coordinating Efforts*.

<sup>57</sup> 16 U.S.C. § 824o–1, (a)(7).

*Disturbance Events* establishes long-lead geomagnetic disturbance planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat for geomagnetic disturbance events.<sup>61</sup> EOP-010-1—*Geomagnetic Disturbance Operations* also requires reliability coordinators to develop geomagnetic disturbance mitigation plans and operating procedures, including specific actions that transmission operators must take based on predetermined geomagnetic disturbance-related conditions.<sup>62</sup>

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyber attacks and other man-made triggers for grid security emergencies. The sun will not intentionally hide preparations for a geomagnetic disturbance event or “prepare the battlefield” by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data that utility personnel need to maintain situational awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of critical and defense critical electric infrastructure.

The relative ease of drafting orders for geomagnetic disturbances makes such efforts a prime starting point for industry–government collaboration. The North American Transmission Forum, in coordination with the ESCC, is already examining opportunities to develop template emergency orders for geomagnetic disturbance events. But the greater degree of difficulty associated with protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of emergency orders to counter such threats. Instead,

DOE and its industry partners should consider pursuing a multitrack development process: at the same time that they seek rapid progress on emergency orders for geomagnetic disturbances, they should *immediately* accelerate the long-lead work that will be required to counter each of the man-made threats that can trigger grid security emergencies.

### Cyber and Physical Attacks

This report focuses on supporting the development of emergency orders to protect and restore grid reliability against cyber and physical attacks. In doing so, the report follows the lead of the premier electric industry exercise of grid resilience, GridEx. As in previous versions of this exercise series, GridEx IV (conducted in November 2017) employed a scenario based on large-scale, combined cyber and physical attacks against the US electric system by a highly capable adversary.<sup>63</sup> Such combined attacks could pose severe threats to nationwide grid reliability, over and above those created by cyber or physical strikes alone. Grid security emergency orders that can help power companies protect and restore reliability against combined attacks will be especially valuable for national security. Orders and implementation plans that can help counter such severe threats will also be useful in lesser contingencies, including cyber-only strikes.

Current US policy priorities focus on the need to strengthen cyber resilience for the power grid and other critical infrastructure. The US *National Security Strategy* warns that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>64</sup> DOE and its partner utilities should prioritize the development of emergency

<sup>61</sup> NERC, *TPL-007-1*.

<sup>62</sup> The standard, however, does not explicitly lay out what those predetermined conditions should be. See NERC, *EOP-010-1*. For an example of geomagnetic disturbance plans, see PJM, *PJM Manual* 13, 69–71.

<sup>63</sup> GridEx includes participation by over one hundred power companies and other components of the electricity subsector. See NERC, *Grid Security Exercise GridEx IV*, vii.

<sup>64</sup> White House, *National Security Strategy*, 12, 27.

orders to counter such attacks, and supplement the mandatory and increasingly stringent cyber critical infrastructure protection standards, as well as voluntary measures that go above and beyond those NERC requirements.<sup>65</sup>

However, orders can also help build resilience against physical attacks on the grid. Since the coordinated attack on the Metcalf substation near San Jose, California, in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high-powered rifles or other weapons. This includes NERC's *CIP-014-2—Physical Security* standard, which outlines the requirements for protecting grid infrastructure from physical attacks.<sup>66</sup> Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide-area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

An adversary would face greater risks when launching physical attacks than cyber attacks. Blowing up transformers and killing workers who are transporting replacement equipment might rapidly escalate conflict with the United States into larger-scale kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries would hide on utility networks, arming and prepositioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages that last far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk-reward calculus in our favor. If orders can help power companies protect their systems from impending physical attacks, especially in partnership with state and local law enforcement agencies, state National Guard personnel, and other sources of assistance, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Adversaries may also simultaneously employ both cyber and physical attacks. Such combined attacks can synergistically disrupt the grid in ways that cyber or physical attacks on their own cannot. For example, as in the response to cyber attacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.<sup>67</sup> However, physical attacks that destroy critical substation components or target utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

The GridEx IV scenario highlighted the unique challenges posed by combined attacks and opportunities to address them. That scenario also assumed that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging that are far more difficult to counter than in any past US power outage.

This report adopts a similarly severe threat for analyzing possible emergency orders. In particular, the report examines how orders can protect or restore grid reliability against the combined use of cyber weapons, physical attacks, and information

---

<sup>65</sup> NERC has mandatory standards for critical infrastructure protection against cyber threats. See "United States Mandatory Standards," NERC.

<sup>66</sup> DOE, *Quadrennial Energy Review*, 4–34; and NERC, *CIP-014-2*.

---

<sup>67</sup> E-ISAC and SANS-ICS, *Analysis of Cyber Attack*, v.

warfare against critical and defense critical electric infrastructure. Of course, separate types of emergency orders will be required for physical and cyber threats. Orders to deploy specific countermeasures against unmanned aerial vehicle attacks on substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead, utilities can also benefit from examining how emergency orders could help them defeat combined attacks, and how they can integrate both cyber and physical defense operations.

The study does not examine options for developing emergency orders against electromagnetic pulse (EMP) attacks. EMP threats pose a significant potential risk to the grid, and a growing (though still relatively small) number of utilities are hardening their critical systems against EMP effects.<sup>68</sup> DOE's EMP strategy provides a valuable framework and approach for managing the risks that EMP threats pose to the grid and other energy systems.<sup>69</sup> DHS's EMP strategy does the same for a broad range of infrastructure sectors.<sup>70</sup> Industry partners such as the Electric Power Research Institute are also making notable contributions to the shared understanding of EMP effects on the grid.<sup>71</sup> However, significant

research is still required to understand the combined effects of EMP wave components on grid hardware and system-wide operations and for cost-effective mitigation options and preparedness planning.<sup>72</sup> As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

## Thresholds for Declaring Grid Security Emergencies<sup>73</sup>

The FPA authorizes the president to declare a grid security emergency when there is "imminent danger" of an attack or when attacks are already occurring. However, the FPA does not further define imminent, nor provide any criteria to help determine whether the anticipated likelihood of an attack is sufficient to warrant an emergency declaration. As will be discussed below, the FPA provides guidance on the potential severity of imminent or ongoing attacks that would constitute a grid security emergency. However, those guidelines are broad and could be subject to starkly different interpretations in future crises.

Some degree of ambiguity is useful. Preserving wide presidential latitude for declaring grid security emergencies will be essential to deal with unforeseen challenges and to avoid locking US crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicize explicit red lines that would trigger a declaration. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay US defensive measures, including the issuance of emergency orders to safeguard the grid. Adversaries might even seek to spoof the president into declaring a grid security emergency when they had no intention of launching an attack—especially if adversaries believed doing so might prompt the issuance of disruptive emergency orders, crash utility stock

<sup>68</sup> In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to geomagnetic disturbances. The early-time component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See EPRI, *Electromagnetic Pulse and Intentional EMI Threats*, 3-3–3-4.

<sup>69</sup> DOE set strategic goals for addressing EMP threats and created an action plan to meet those goals. DOE, *Electromagnetic Pulse Resilience Action Plan*. The fiscal year 2017 National Defense Authorization Act directed DHS to create a similar strategy, which is currently in draft form. See National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328. The EPRI continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse*.

<sup>70</sup> DHS, *Strategy for Protecting and Preparing*.

<sup>71</sup> EPRI, *Electromagnetic Pulse and Intentional EMI Threats*.

<sup>72</sup> INL, *Strategies, Protections, and Mitigations*.

<sup>73</sup> The analysis in this section builds on the findings of Stockton, "Thresholds."



prices, or incite public panic in ways that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events that emergency orders should be designed to help counter.<sup>74</sup> Federal officials could also find it useful to have decision criteria to help frame their own internal deliberations and recommendations to the president. In an intense crisis, ambiguities in the FPA could fuel disagreements among the president's advisors as to whether the threat of attack was sufficiently severe to declare a grid security emergency. Developing a decision framework to support the declaration process could facilitate consensus-building and provide a structured way to integrate data on attack indicators. However, in adopting such a framework, it would also be prudent to avoid revealing any specific declaration triggers or thresholds for adversaries to exploit in their attack planning.

The section that follows examines two factors that a decision framework might encompass: the likelihood of an attack occurring and its potential consequences. This section also examines how improved information sharing between government agencies and power companies can support these assessments and recommends industry–government consultations in the declaration process that go beyond the existing provisions of the FPA.

### **Determining When Attacks Are Imminent: Criteria for Declaring Grid Security Emergencies**

In key respects, the BPS is under cyber attack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant advanced persistent threats on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS networks, secrete malware

designed to disrupt grid operations, and conduct other malicious activities to prepare for possible attacks on critical system components.<sup>75</sup> PJM Interconnection's former CEO Terry Boston recently stated that the company experiences three thousand to four thousand hacking attempts *every month*.<sup>76</sup> Penetration efforts on a similarly massive scale are likely occurring against BPS entities across the United States. While many of these efforts target information technology systems not directly involved in operating the grid, malware implants on operational technology systems are increasingly frequent and sophisticated.<sup>77</sup> And, as in the case of BlackEnergy and other campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.<sup>78</sup> The net result, according to US director of national intelligence Dan Coats: "Today, the digital infrastructure that serves this country is literally under attack."<sup>79</sup>

Of course, there is a huge gulf between implanting destructive malware on the grid and using that malware to create blackouts. The Trump administration has promised to impose "swift and costly consequences" on foreign governments and other actors who undertake "significant malicious cyber activities" against US critical infrastructure.<sup>80</sup> Attacks that create massive power outages and jeopardize US national security would be especially likely to provoke such a response. However, the president does not need to wait for blackouts to occur before declaring

<sup>75</sup> "Alert (TA18-074A)"; "Alert (TA17-293A)"; Defense Science Board, *Task Force on Cyber Deterrence*, 4; and ICF International, *Electric Grid Security and Resilience*, 19.

<sup>76</sup> Dougherty, "Biggest U.S. Power Grid Operator Suffers Attacks."

<sup>77</sup> "Alert (TA17-293A)"; and "Alert (TA18-074A)."

<sup>78</sup> BlackEnergy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of BlackEnergy inflicted the 2016 blackout on Ukraine. "Alert (ICS-ALERT-14-281-01E)."

<sup>79</sup> Barnes, "Warning Lights."

<sup>80</sup> White House, *National Security Strategy*, 13.

<sup>74</sup> Paradise et al., "ISO-RTO Council Comments," 2.



a grid security emergency. The “imminent danger” of attack is sufficient to declare an emergency and for the secretary to issue orders to help utilities ramp up their defenses.

Implants of new, potentially devastating malware across the electric grid could help the president make such a determination, particularly if other warning indicators suggest that cyber attacks are becoming increasingly likely. The geopolitical context in which cyber attacks might occur provides one such indicator. It is (barely) conceivable that adversaries will launch a “bolt from the blue” attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region and attack the grid to disrupt the deployment of US forces to the region or to achieve other military and political goals.<sup>81</sup> Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause multistate blackouts, should carry greater weight in a crisis environment.

Policy makers should consider developing a framework to assess whether these cyber preparations help justify the declaration of a grid security emergency. The US Office of the Director of National Intelligence (ODNI) has issued a cyber threat framework that could support such development efforts. The ODNI notes that government agencies, academia, and the private sector are using over a dozen analytic models to categorize cyber threats and identify changes in the activities of cyber adversaries. ODNI’s framework is intended to provide a common basis for characterizing threat activity to support analysis and senior-level decision-making.<sup>82</sup> Figure 2 illustrates the cyber threat framework.

<sup>81</sup> The section on preattack grid security emergency declarations examines these national security-related issues and their implications for designing emergency orders.

<sup>82</sup> “Cyber Threat Framework,” ODNI; and ODNI, *Common Threat Framework*, 5.

The initial stage of adversary activity is to prepare for conducting malicious activity. Adversaries then engage and establish presence on targeted systems, allowing them to “operate at will.” In the final stages, attackers seek to destroy grid hardware, software, and/or data, and prepare to conduct follow-on operations as needed to magnify the extent and duration of their disruptive effects.<sup>83</sup>

If adversaries were to suddenly make new moves into the penultimate phase (operate at will) during an intense political crisis or regional confrontation, evidence that they had done so could help the president determine whether attacks were imminent. Other independent sources of data could provide additional context for assessing adversary moves toward more threatening preattack stages. James Miller, former undersecretary of defense for policy, notes that “the United States devotes massive resources to human and technical intelligence collection of our potential adversaries.”<sup>84</sup> Such indicators could contribute to overall assessments of attack imminence.

Policy makers might also supplement the cyber threat framework with specialized attack models for the industrial control systems and other grid components that are crucial for electric system operations. The Industrial Control System Cyber Kill Chain provides an especially promising opportunity to do so. The kill chain identifies the specific sequenced phases that adversaries execute to conduct attacks that inflict predictable physical effects on grid equipment and operations.<sup>85</sup> Stage 1 begins with planning and reconnaissance against

<sup>83</sup> ODNI, *Common Threat Framework*, 13, 16.

<sup>84</sup> Miller, “Cyber Deterrence.”

<sup>85</sup> The Industrial Control System Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin in 2011 to “help the decision-making process for better detecting and responding to adversary intrusions.” The Industrial Control System Cyber Kill Chain tailors that decision-making tool for industrial control system-specific cyber threats and consequences. See Assante and Lee, *Industrial Control System Cyber Kill Chain*.

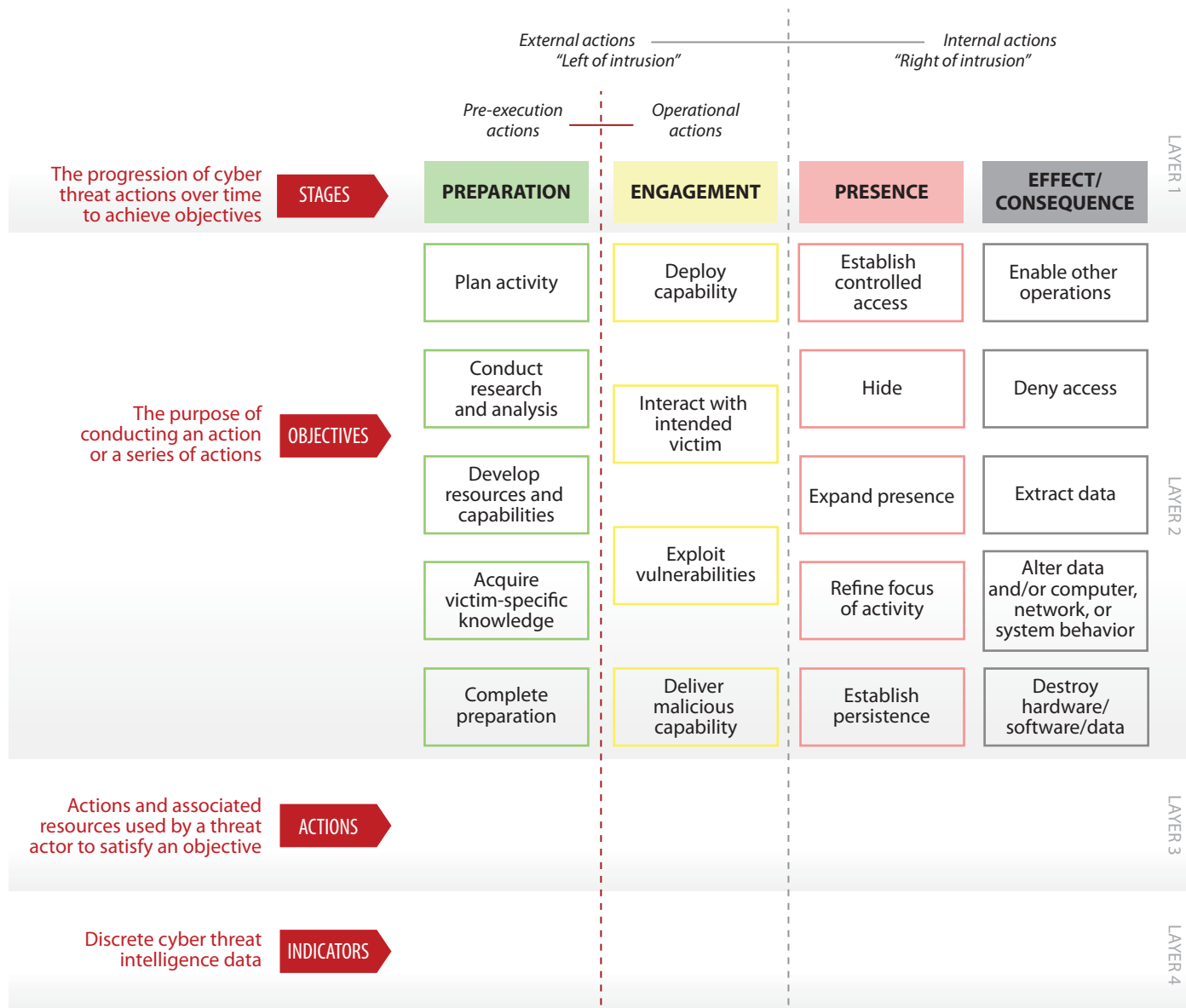


Figure 2. ODNI Cyber Threat Framework

industrial control system networks and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing attack capabilities, and—ultimately—executing the attack. Evidence of an adversary's position along this kill chain could help support decision-making on the imminence of potential attacks, with the final phases posing the most proximate indications that an adversary is poised to strike the grid.

### Potential Attack Consequences

The imminence of an attack provides only one possible criterion for declaring a grid security emergency. A second would be the potential consequences of the attack. Indeed, when Congress defined grid security emergencies in the FPA, legislators established at least implicit, consequence-based thresholds for declaring an emergency. The FPA defines grid security emergencies as occurring when attacks that are imminent or under way "could disrupt the

	General Definition	Observed Action	Intended Consequence
Level 5: Emergency (Black)	<i>Poses on imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons</i>	Effect	Cause physical consequence
Level 4: Severe (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties</i>	Presence	Damage computer and networking hardware
Level 3: High (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>	Engagement	Corrupt or destroy data  Deny availability to a key system or service
Level 2: Medium (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Steal sensitive information
Level 1: Low (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Commit a financial crime
Level 0: Baseline (White)	Unsubstantiated or inconsequential event	Preparation	Nuisance denial of service or defacement

Figure 3. Elements of the Cyber Incident Severity Schema

operation” of devices or networks that are “essential to the reliability of critical electric infrastructure or defense critical electric infrastructure.”<sup>86</sup>

However, the FPA does not clarify the extent of disruption that should trigger the declaration of an emergency. Some grid resilience stakeholders have expressed concern that policy makers might set the threshold too low, and declare grid security emergencies for minor incidents. For example, the ISO/RTO Council proposes that the use of emergency orders in such an emergency “should be reserved for true widespread emergencies.”<sup>87</sup> But

neither Congress nor DOE have yet specified what higher-level thresholds might be appropriate.

One approach to account for the potential consequences of an attack would be to leverage existing federal criteria for categorizing cyber events by the severity of their effects. The definition of “significant cyber incidents” in Presidential Policy Directive 41, *United States Cyber Incident Coordination*, provides a starting point to do so. Under the directive, significant cyber incidents are those that are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or

<sup>86</sup> 16 U.S.C. § 824o-1, (a)(7).

<sup>87</sup> Paradise et al., “ISO-RTO Council Comments,” 2.

public health and safety of the American people.”<sup>88</sup> Policy makers could apply this demonstrable-harm standard to support decisions on whether to declare a grid security emergency. If officials determine that a cyber attack is likely to inflict such harm, their finding would provide a compelling justification for making an emergency declaration.

The December 2016 *National Cyber Incident Response Plan*’s cyber incident severity schema offers a still more detailed basis to assess attack consequences. The schema (Figure 3) serves as “a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments” and agencies.<sup>89</sup> Policy makers could use the schema to help develop consequence-based criteria for declaring grid security emergencies. For example, if assessments suggest that an attack is likely to create a “level 5 emergency,” which poses “an imminent threat to the provision of wide-scale critical infrastructure services, national [government] stability, or to the lives of U.S. persons,” the declaration of a grid security emergency should be near-automatic. Level 4 events would also be very strong candidates for justifying such declarations. However, as with all such criteria, the president should also retain the latitude to make declarations for less severe incidents (for example, the disruption of a cluster of major defense installations).

One advantage of leveraging these government-wide standards is that doing so can help integrate decisions on grid security emergencies into the broader US system for incident response. As officials update the *National Cyber Incident Response Plan* and its supporting severity schema, valuable opportunities will emerge to ensure that grid security emergency declarations and operations are part of a broader, multisector approach to strengthening infrastructure preparedness.

### **Grid-Specific Criteria for Assessing Attack Consequences: Building on Standards for Adequate Levels of Reliability**

If policy makers rely only on general, government-wide decision criteria, they will miss opportunities to take advantage of the electric industry’s standards for assessing the severity of threats to grid reliability. NERC has carefully defined what constitutes adequate reliability for the power grid, as well as the types of large-scale reliability failures that owners and operators need to prevent. If utilities and government agencies have the data and analytic tools necessary to determine whether adversaries’ attacks will create such failures, their assessments could provide valuable input into decisions on declaring grid security emergencies.

The 2003 Northeast blackout spurred NERC’s efforts to define adequate levels of grid reliability and specify the types of system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over wide areas of the United States and Canada, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The 2005 amendments required FERC to certify an electric reliability organization, which will have “the ability to develop and enforce . . . reliability standards that provide for an adequate level of reliability of the bulk-power system.”<sup>90</sup> However, the FPA never defined *adequate level of reliability*; that task was left to the electric reliability organization.

When NERC became the electric reliability organization in 2006, defining the adequate level of reliability was one of its first initiatives. NERC’s board of trustees approved an initial definition for the “characteristics of a system with an adequate level of reliability” in 2008, which was updated in 2013.<sup>91</sup> Three components of NERC’s definition—cascading failures, uncontrolled separation, and instability—are

<sup>88</sup> Obama, *United States Cyber Incident Coordination*.

<sup>89</sup> DHS, *National Cyber Incident Response Plan*, 29–30.

<sup>90</sup> 16 U.S.C. § 824o, (c)(1).

<sup>91</sup> NERC, *Technical Report*, 17.

especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS.<sup>92</sup>

The sections that follow examine these three components, the reliability failures they can entail, and implications for declaring grid security emergencies. Subsequent portions of the report analyze options to develop emergency orders tailored to prevent such failures. However, in grid security emergencies, risks of all three types of failures might emerge in rapid succession and would be inextricably linked.

**Cascading failures.** NERC defines cascading as “the uncontrolled successive loss of system elements triggered by an incident at any location.” Such cascading “results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.”<sup>93</sup> NERC’s definition states that a system is adequately reliable if the system will not experience cascading failures when struck by lightning or affected by other frequent, predictable incidents (i.e., “predefined Disturbances”). But more severe events have caused instabilities that led to cascading in the past and may do so again—especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout illustrates the speed with which failures can cascade. That blackout, which affected approximately fifty million people across the United States and Canada, started with a relatively minor incident. On a hot day in August, multiple 345-kilovolt transmission lines tripped after sagging into overgrown trees. With proper situational awareness, operators might have been able to take actions to handle such a contingency, but failures in

the utility’s control room alarm processor resulted in operators being entirely unaware of the problem. In an unfortunate coincidence, the utility’s reliability coordinator also had computer problems and lacked the visual tools necessary to support grid operators.<sup>94</sup> These failures shifted power flows to a system of 138-kilovolt lines, which were unable to handle the added current flows, and overloaded the last remaining 345-kilovolt path into the area, beginning the major, uncontrollable cascading sequence.<sup>95</sup> This sequence tripped over five hundred generating units and four hundred transmission lines in only eight minutes—with most of these failures occurring *in the last twelve seconds* of the cascade.<sup>96</sup>

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversarial attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying critical generation and transmission nodes; alter protective relay settings so that grid components trip offline (or fail to do so) in ways that intensify the outages; deny grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and take other measures designed to produce cascading failures.<sup>97</sup> Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe—particularly by denying or corrupting situational awareness data.

The imminent danger or occurrence of adversary-induced cascading outages could be a criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt

<sup>92</sup> See section 215 of the FPA, which defines *reliable operation* as “operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” 16 U.S.C. § 824o, (a)(4).

<sup>93</sup> NERC, “Informational Filing,” 1, 7.

<sup>94</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>95</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>96</sup> NERC Steering Group, *Technical Analysis of Blackout*, 109.

<sup>97</sup> Cherepanov and Lipovsky, “Industroyer”; Sistrunk, “ICS Cross-Industry Learning”; “Alert (TA17-163A)”; and Dragos, *CRASHOVERRIDE*, 24.



the operation of grid devices and networks essential to critical and defense critical electric infrastructure—on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

**Uncontrolled separation.** NERC defines uncontrolled separation as “the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss.”<sup>98</sup> Severe events “resulting in the removal of two or more BES elements with high potential to cascade” can produce uncontrolled separation.<sup>99</sup>

Uncontrolled separation almost always occurs in conjunction with cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands that “quickly became unstable after the massive transient swings and system separation” because there was insufficient generation within the islands to meet electricity demand.<sup>100</sup> Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.<sup>101</sup> In the 1982 West Coast blackout, loss of 500-kilovolt lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, dividing the system into four unplanned islands.<sup>102</sup> A similar blackout in the same region in 1996, triggered by multiple major transmission line outages, again separated the Western Interconnection into four electrical islands

“with significant loss of load and generation.”<sup>103</sup> The onset of adversary-induced uncontrolled separation would provide a clear-cut basis for declaring the existence of a grid security emergency, if cascading failures had not already prompted the president to make such a determination.

**Instability.** NERC defines system instability as “the inability of the Transmission system to remain in synchronism . . . characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES.”<sup>104</sup> The BES can experience frequency, voltage, or angular instability—though none should occur during normal operating conditions.<sup>105</sup>

Severe natural hazards and other disturbances can create temporary instabilities. Grid protection systems and operational protocols typically mitigate their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, the transmission system may experience large power swings if BPS generators accelerate or decelerate too much during a disturbance, causing transmission lines to trip and generators to go out of step and trip offline, and resulting in further acceleration and deceleration—or both.<sup>106</sup> Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread cascading failures. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur. Corrupting or disabling protection systems could also make critical grid components vulnerable to physical damage from enemy-induced power surges.

<sup>98</sup> NERC, “Informational Filing,” 6.

<sup>99</sup> NERC, “Informational Filing,” 13.

<sup>100</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 75.

<sup>101</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 104.

<sup>102</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 105.

<sup>103</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 106.

<sup>104</sup> NERC, “Informational Filing,” 6.

<sup>105</sup> NERC, “Informational Filing,” 1–2.

<sup>106</sup> NERC, “Informational Filing,” 6.

Evidence that adversaries were taking preparatory measures to create widespread instabilities could help the president determine that a grid security emergency exists.

However, it may be difficult to predict whether an impending attack will create such failures. The first requirement to do so will be to determine the extent to which adversaries have embedded advanced persistent threats or established other means of attack across the grid—a task that adversaries will complicate by attempting to hide their malware from detection. The next step will be to rapidly characterize these threats, assess the vulnerability of utility systems to them, and predict the consequences for grid reliability if the enemy strikes. Such assessments will also need to account for system-wide effects involving the interaction of multiple adversary-induced disruptions, which may compound and reinforce instabilities in ways that are difficult to predict. PJM Interconnection, LLC, the regional transmission operator for much of the Mid-Atlantic and some neighboring states, recently noted that “additional study is needed to better understand the expected impacts of a large-scale cyber-attack.”<sup>107</sup> Given these challenges, it may be difficult to fully predict the potential impact of cyber attacks on grid reliability until attacks are well under way.

But it could also be risky to wait until attacks are occurring to declare a grid security emergency. In the 2003 Northeast event, for example, cascading blackouts spread across vast areas in seconds. If the president delays declaring a grid security emergency until cascades are under way, emergency orders designed to help prevent their spread may come too late. A better option might be to make an early decision based on imperfect assessments, especially if (as this report recommends) DOE can issue preattack emergency orders that will bolster grid defenses without disrupting normal electric service.

In particular, the president could consider declaring a grid security emergency if (1) an attack appears to be increasingly likely, and (2) assessments indicate that the impending attack may create cascading blackouts or other widespread instabilities. Figure 4 illustrates one option for developing a decision support framework that accounts for the likelihood and potential consequences of an attack. The vertical axis depicts the ODNI cyber threat framework’s four stages of adversary actions, from potential attack preparations to actual strikes against the grid. An adversary’s sudden, large-scale moves up this axis—especially in the context of a severe international crisis—could help the president determine that an attack is impending. The horizontal axis represents the risk that if an attack occurs, the grid will experience cascading failures and other widespread instabilities that would inflict demonstrable harm to national security, the economy, or public health and safety. Attacks that pose little or no risk of cascading blackouts might not warrant the declaration of a grid security emergency.

However, systemic threats to grid reliability are far from the only consequence-based criteria that the president might want to consider. More narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security, such as the National Capital Region, might be sufficient to declare a grid security emergency. Policy makers could develop more refined decision frameworks to account for a broad array of consequence thresholds, as well as further criteria for assessing attack imminence.

## Data Sharing and Consultations with Industry

The electric industry can provide data and analytic support to help the president and other officials decide whether to declare a grid security emergency. Power companies will have direct access to the malware that adversaries implant on their networks, and will be well positioned to assess the potential

<sup>107</sup> PJM, “Comments and Responses,” 35.

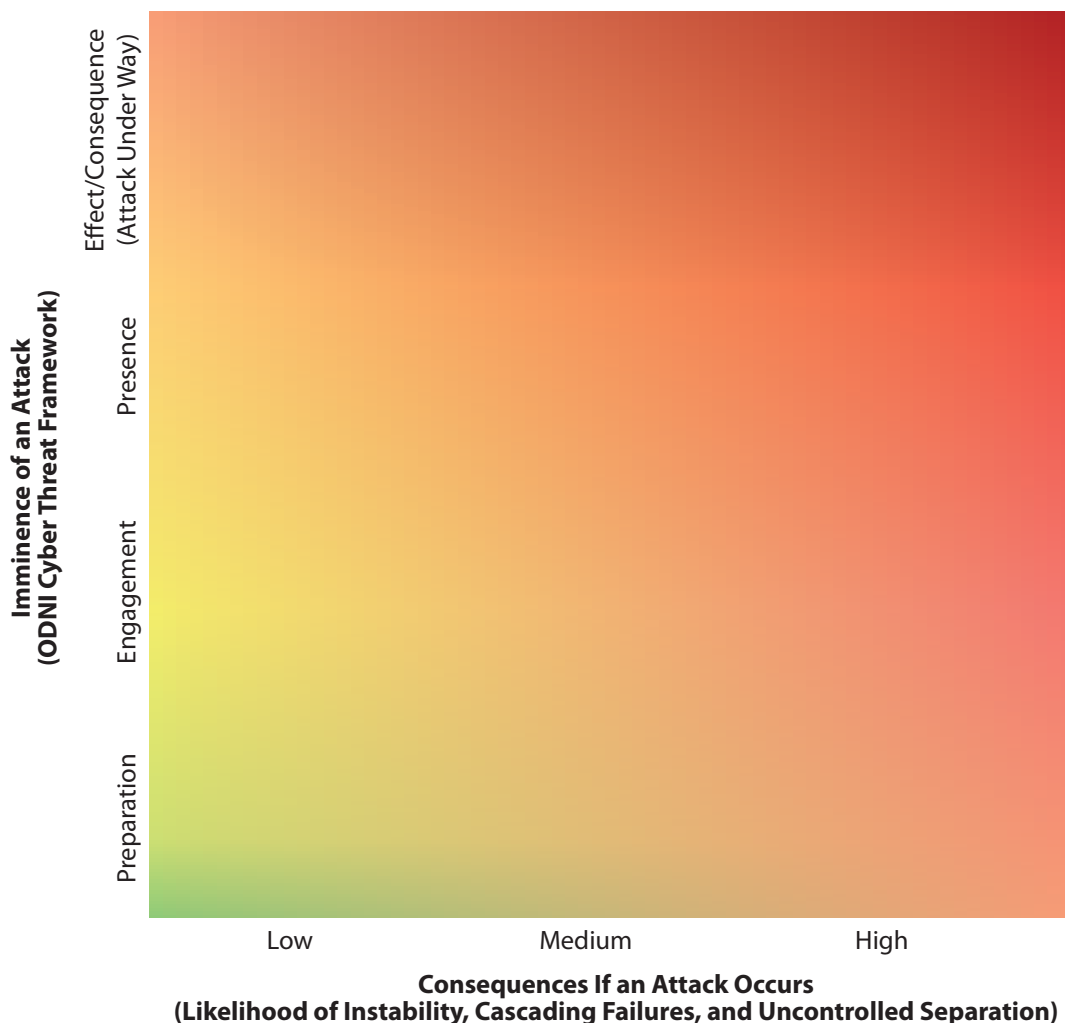


Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies

impact of various attack vectors on their systems and on the grid as a whole.

Government agencies and cyber contractors can help utilities target searches for this malware and provide additional value for the declaration process. If a regional crisis or other geopolitical factors increase the risk of cyber attacks on the grid, agencies should be prepared to ramp up information sharing with BPS entities, especially in terms of specific signatures or other threat indicators to search for in utility networks, logs, and critical equipment.

Industry and government should also explore how ongoing threat detection and analysis initiatives could directly help assess the imminence and

potential consequences of attacks. For example, DOE has projects under way to bolster situational awareness for operational technology networks that could be applied to support such assessments. The department is developing capabilities to monitor traffic on operational technology networks via the Cybersecurity for the Operational Technology Environment project.<sup>108</sup> Other department-funded projects could prove useful for the emergency declaration process as well.<sup>109</sup>

<sup>108</sup> DOE, *Multiyear Plan*, 23.

<sup>109</sup> See, for example, the Containerized Application Security for Industrial Control Systems, Survivable Industrial Control Systems, and Research Exploring Malware in Energy Delivery Systems projects. “Sandia’s Grid Modernization Program

Utilities and DOE might also refine ongoing information sharing initiatives to directly support the emergency declaration process. For example, DOE's Cybersecurity Risk Information Sharing Program is a public-private partnership to build bidirectional situational awareness and facilitate classified and unclassified information sharing.<sup>110</sup> DOE's 2018 cybersecurity plan launched additional activities to advance industry participation in the program, as well as its analytic tools and capabilities.<sup>111</sup> The program is managed by NERC and the E-ISAC, which play an integral role in sharing information and establishing situational awareness within the electricity subsector.<sup>112</sup> In addition, FERC recently issued a proposed directive for NERC to expand reporting requirements for cyber incidents, including for those that "might facilitate subsequent efforts to harm the reliable operation of the bulk electric system."<sup>113</sup> All of these efforts could be integrated to support assessments of the likelihood and potential consequences of attacks.

DHS's May 2018 cybersecurity strategy provides a broader approach to expand information sharing. Most important, the strategy could enable data from other infrastructure sectors to support the declaration process, especially from communications systems and other sectors that support power restoration operations. The strategy also calls for the expansion of automated mechanisms to receive, analyze, and share cyber threat indicators, defensive measures, and other cybersecurity information with critical infrastructure and other key stakeholders.<sup>114</sup>

Such automated sharing mechanisms will be vital to accelerate the identification and assessment of malware that could pose imminent threats to grid reliability. DHS's Automated Indicator Sharing capability "enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed."<sup>115</sup> This bidirectional information sharing will limit an adversary's ability to compromise multiple systems with the same malicious code. The Defense Advanced Research Projects Agency is also working on new technologies to protect the grid. In particular, the agency's Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is working with companies to develop prototype capabilities for improving attack detection, response, and forensics support.<sup>116</sup> Moreover, as automated malware detection and analytic techniques improve, utilities may be able to speed their evaluation of potential intrusions and slash the number of false positives that current detection systems generate.<sup>117</sup> All of these initiatives should be leveraged to help the president determine whether to declare a grid security emergency.

Policy makers should also consider preplanning to consult with grid owners and operators in the declaration process. The FPA leaves the president with sole authority to declare a grid security emergency. If a potential emergency surfaced, the president would almost certainly draw on the expertise and recommendations of the secretary of energy, as well as other members of the National Security Council and supporting agencies. But power companies and their industry organizations will also have perspectives on operational and technical issues that could prove valuable for assessing potential attacks.

---

Newsletter," Sandia National Laboratories; and "REMEDIYS," Cyber Resilient Energy Delivery Consortium.

<sup>110</sup> "Energy Sector Cybersecurity Preparedness," DOE.

<sup>111</sup> DOE, *Multiyear Plan*, 23.

<sup>112</sup> "Electricity Information Sharing and Analysis Center," NERC.

<sup>113</sup> FERC, *Cyber Security Incident Reporting Reliability Standards* (161 FERC ¶ 61,291), 2.

<sup>114</sup> DHS, *Cybersecurity Strategy*, 13.

---

<sup>115</sup> "Automated Indicator Sharing (AIS)," US-CERT.

<sup>116</sup> Douris, "DARPA Research."

<sup>117</sup> Ucci, Aniello, and Baldoni, "Survey on Machine Learning," 1:5; McElwee et al., "Deep Learning"; and McElwee, "Probabilistic Cluster."

Neither the FPA nor the grid security emergency rule explicitly provide for consultations with industry on whether to declare a grid security emergency. The FPA calls for consultations “to the extent practicable” before the secretary issues emergency orders.<sup>118</sup> But there are no equivalent provisions to include industry input in the emergency declaration process.

Industry and government partners should explore options to provide for such consultations, preferably by leveraging existing mechanisms under the ESCC and E-ISAC. As with consultations on issuing orders, urgent circumstances could shorten or preclude opportunities for government dialogue with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of “bolt from the blue” attacks. Nevertheless, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be invaluable for determining whether (and when) to declare a grid security emergency.

## Grid Security Emergency Phases and Order Design Options

DOE and its industry partners should consider designing emergency orders for three potential phases of grid security emergencies. First, if the president determines that there is an imminent danger of an attack, the secretary should be ready to issue preattack orders that help utilities protect grid reliability. Second, once attacks are under way, the secretary could issue orders to reduce the risk of cascading failures or other widespread disruptions of electric service. Third, as utilities begin to restore grid reliability, orders could help utilities replace damaged equipment and counter adversary efforts to disrupt restoration operations.

Orders for each phase of a grid security emergency will differ not only in terms of when the secretary would issue them but also in the degree to which they

will disrupt normal electric service. Some orders, such as staffing up emergency operations centers before an attack occurs, would leave customers unaffected. In contrast, orders for prioritized load shedding could temporarily halt service to many customers—but could also greatly reduce the risk that instabilities will lead to cascading blackouts.

Figure 5 provides examples of orders that vary in the degree of disruption they would inflict on normal service, and also in the way they would meet the phase-specific challenges of grid security emergencies. The analysis that follows examines each of them (and other possible orders) in greater detail.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, emergency orders for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are under way. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies “stop the bleeding” from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are under way.<sup>119</sup> Adversaries may also launch follow-on attacks once utilities begin focusing on restoration. Emergency orders to help utilities repel such attacks could become essential components of the restoration process.

<sup>118</sup> 16 U.S.C. § 824o–1, (b)(3).

<sup>119</sup> In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is fully restored to pre-event conditions) as the “new normal”—characterized by “degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months.” See Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.



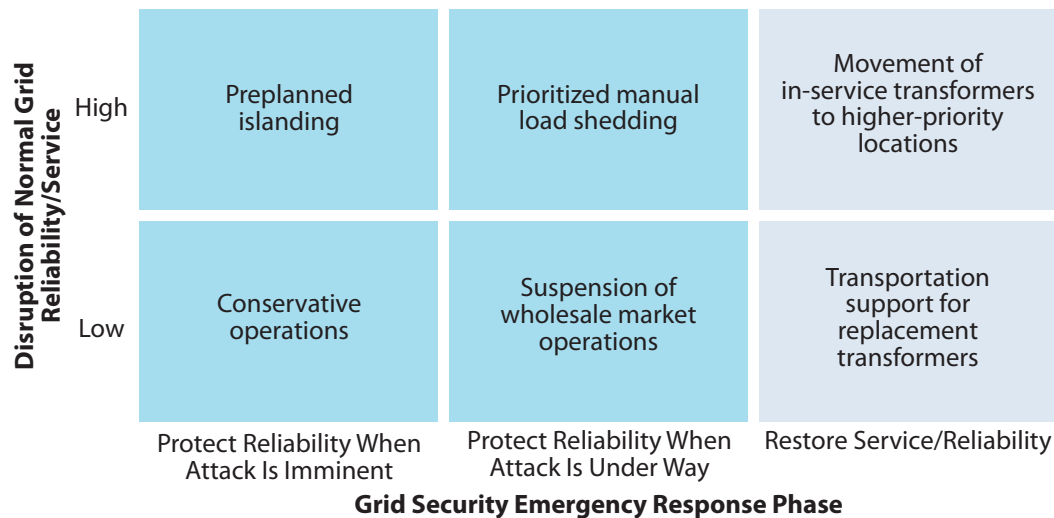


Figure 5. Emergency Order Matrix: Examples of Order Designs

DOE and its partners will need flexibility to deal with the overlapping phases of grid security emergencies. Nevertheless, being able to categorize potential orders in terms of when they would likely be issued and which phases of emergency operations they could support can help establish a systematic process for developing orders.

Creating emergency orders for all three phases can also help utilities and DOE integrate the orders into seamless, multiphase operational plans for grid security emergencies. As intense regional crises or other events elevate the risk of attacks on the grid, it will be prudent to preplan for the issuance of emergency orders for multiple grid security emergency phases. Orders for preattack measures such as conservative operations would be issued first if attacks are deemed imminent. At the same time, however, DOE and the utilities subject to emergency orders should be using any available warning time to prepare for the issuance and implementation of orders for the midattack and restoration phases.

## Preattack Options

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal

with these ambiguities is to delay the declaration of a grid security emergency until blackouts begin; doing so would forego the benefits of issuing preattack emergency orders. It may be possible to develop orders that will offer significant benefits if adversaries strike yet also have little or no impact on normal service—thereby offering “no-regrets” options to employ when the likelihood of an attack remains uncertain. Industry and government partners should also explore options for the preattack phase that would be more disruptive but also offer potentially far-reaching benefits. These two options occupy the left-hand column in Figure 5.

Conservative operations that utilities employ against natural hazards provide a model for protecting the grid in ambiguous preattack situations. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects and prepare for possible response and restoration operations if grid infrastructure is damaged.<sup>120</sup> For

<sup>120</sup> Conservative operations are not defined in the NERC glossary of terms. However, many reliability coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken to “implement

example, reliability coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.<sup>121</sup> Power companies may also cancel noncritical generation and transmission maintenance activities; reduce transfer limits to give the transmission system extra “slack”; and staff their backup control centers, critical BPS substations, and other vital facilities to set the stage for emergency operations as hurricanes approach.<sup>122</sup>

A defining feature of these frequently used conservative operations is that they do not disrupt normal service to customers. Their negligible service impact makes them more viable to implement when the storm’s path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the US coast. Instead, they provide a wide “cone of uncertainty” that becomes increasingly narrow as the hurricane approaches. Utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other conservative operations. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these operations do not affect normal service to customers enhances the willingness of utility leaders to order their implementation while the storm track remains uncertain.

---

additional actions to ensure the BES remains reliable in the face of the additional threats” when “events, conditions, or circumstances may put the Bulk Electric System (BES) at an increased level of risk, compared to normal operating conditions.” See PJM, “Conservative Operations,” 3. Similarly, the Western Electricity Coordinating Council, defines conservative systems operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets “are restricted and managed in order to maintain or restore reliability of the power system from the negative influence of a triggering event or condition.” See Western Electricity Coordinating Council, “Conservative System Operations,” 4.

<sup>121</sup> PJM, “Conservative Operations,” 3.

<sup>122</sup> PJM, “Conservative Operations,” 9.

Industry and government partners should borrow from this model to develop orders for preattack conservative operations against cyber and/or physical attacks. Some have already begun to do so. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting conservative operations to meet the specialized challenges posed by cyber and physical threats.<sup>123</sup> This preparation will be extremely helpful as potential attacks loom. As a regional confrontation or other precipitating crisis intensifies, it is conceivable that the US intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. However, it is much more likely that ambiguities will persist about whether the adversary will actually attack and risk a devastating US response. To ensure that sufficient time is available to implement conservative operations, the secretary may need to order the initiation of such measures when enemy intentions remain uncertain—and when warning indicators may turn out to be false.

Many of the conservative operations that will bolster resilience against adversary attacks would be similar to those developed for natural hazards. For example, preattack emergency orders might direct BPS entities to increase generation reserves and/or re-dispatch resources out of least-cost operations. Other orders might be threat specific: for example, to intensify scrutiny of operational technology networks for malware and implement government-vetted counter-measures in ways that give utilities sufficient latitude to account for their unique system characteristics.

The common denominator for all such options: if the secretary issues orders for BPS entities to adopt conservative operations and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented the orders.

---

<sup>123</sup> See, for example, PJM, *PJM Manual* 13, 73; Lucas, “Conservative Operations”; and SERC, *Conservative Operations Guidelines*.

However, because so many utilities already have robust plans and capabilities to protect their systems from imminent threats, close government–industry coordination will be required to ensure that emergency orders actually assist grid defense rather than function as speed bumps or useless distractions. Reliability coordinators and other grid operators serve as the pointy end of the spear for protecting grid reliability. Mandatory NERC standards require BPS entities to maintain voltage stability, automatic load shedding schemes, and contingency reserves for disturbances.<sup>124</sup> NERC standards also require transmission operators to “develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area.”<sup>125</sup> Balancing authorities have similar requirements to manage generating and demand-side resources in their service areas.<sup>126</sup> These plans are exercised, tested, and frequently updated to bolster their effectiveness for actual emergencies. While many of NERC’s mandatory standards apply when disturbances begin to occur, BPS entities are spring-loaded to implement conservative operations the moment potential hazards begin to emerge.

If major grid disruptions occur, BPS entities will not sit on their hands and wait for the president to declare a grid security emergency and the secretary to issue emergency orders. Indeed, DOE does not contemplate that they will. In the final grid security emergency rule, the department states that the declaration of a grid security emergency “does not preclude electric utilities from taking time-sensitive action to secure the safety, security, or reliability of the electric grid prior to the issuance of an emergency order.”<sup>127</sup>

DOE and its partners can design emergency orders to help supplement and support such industry-led operations. For example, government agencies may acquire highly classified indicators that an attack is imminent. Declaring a grid security emergency and issuing emergency orders for conservative operations could ensure that utilities bolster their preparedness against such attacks on a consistent, nationwide basis, including those utilities that had not yet identified a need to act. Orders to help power companies ramp up and target searches for specific types of malware could supplement utilities’ defensive operations as well. The secretary might also issue orders to ensure that such industry operations benefited from the FPA’s regulatory protections and cost-recovery provisions.

### More Disruptive Preattack Options

Many utilities are also prepared to take pre-event emergency measures that will significantly disrupt normal electric service, yet also offer benefits far beyond those that conservative operations can provide. For example, power companies can selectively halt electric service on warning of catastrophic storm surges. If seawater hits systems that are still carrying electricity, transformers and other difficult-to-replace grid components will suffer catastrophic physical damage. In 2012, weather forecasters warned that Superstorm Sandy might produce storm surges that would inundate critical substations and underground electrical equipment in lower Manhattan. Consolidated Edison’s team made the politically difficult decision to prevent such damage by preemptively cutting of power to the area. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.<sup>128</sup> Moreover, Consolidated Edison limited the shutdown’s disruptiveness by notifying customers hours earlier that the utility might halt service and by already having plans in place to prioritize the

<sup>124</sup> See, for example, NERC, *VAR-001-4.2*; NERC, *Standard PRC-006-3*; NERC, *PRC-010-2*; and NERC, *BAL-002-2(i)*.

<sup>125</sup> NERC, *EOP-011-1*, R1.

<sup>126</sup> NERC, *EOP-011-1*, R2.

<sup>127</sup> DOE, “RIN 1901–AB40,” 1177.

<sup>128</sup> Miller, “Con Edison Shuts off Power.”

restoration of service to hospitals, water-pumping stations, and other critical facilities.<sup>129</sup>

BPS entities continue to use “shutdown on warning” as an effective tool to avoid equipment damage against severe weather and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent equipment damage and speed up restoration. Generation owners similarly chose to shut down or evacuate some generating units in the storm’s projected path.<sup>130</sup>

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and heating and air conditioning systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

DOE and its electricity subsector partners should consider developing emergency orders that offer a similar set of risks and rewards. However, doing so will entail problems beyond those associated with protecting the grid against natural hazards. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an adversary will actually pull the (cyber) trigger and whether attacks are likely to cause demonstrable harm to the US economy, national security, or public health and safety. Measures developed for natural hazards may also offer uncertain benefits against imminent cyber and physical attacks. For example, further analysis will be required to determine whether and how preattack grid shutdowns might help counter specific cyber threats, including attacks that disable

protection systems to facilitate equipment-damaging power surges.

Other disruptive emergency orders could counter a broader range of threats but entail major (and perhaps insurmountable) problems for nationwide employment. The upper left-hand box in Figure 5 offers a prime example of such options: preplanned power islanding. Microgrids offer the most familiar means of establishing power islands.<sup>131</sup> A growing number of military bases, universities, and major hospitals have sufficient generation and other electric infrastructure on-site so that if adversaries black out the surrounding grid (or pose an imminent danger of doing so), those facilities can separate from the grid and operate independently as power islands.

However, microgrids do not offer “bulletproof” power resilience. Cyber adversaries are sure to treat on-base electric infrastructure, including renewable generation assets, as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas-fired generators, the power they provide is only as resilient as the gas transmission and distribution systems that supply them—and cyber threats to natural gas systems are rapidly escalating.<sup>132</sup> Moreover, building microgrids requires extensive investment in grid infrastructure. Investment demands will be especially heavy if installations want to serve not only the critical loads within their perimeters but also the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to building microgrids, power companies are also analyzing ways to establish emergency power islands with less infrastructure investment. One particular option being explored by GridEx participants is to preplan to establish large

<sup>129</sup> DiSavino and Sheppard, “ConEd Cuts Power.”

<sup>130</sup> NERC, *Hurricane Harvey*, v.

<sup>131</sup> DOE’s definition of microgrids: “A microgrid is a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously.” “The Role of Microgrids,” DOE.

<sup>132</sup> DOE, *Quadrennial Energy Review*, 7-7; and Parfomak, *Pipelines*, 2-3.



power islands by using existing grid infrastructure within their boundaries. Utility personnel have noted that they might be able to use legacy balancing areas as a starting point to establish island boundaries. On warning of an imminent attack or under other extraordinary circumstances, utilities would separate a power island from the surrounding grid and operate independently to serve critical loads within it. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, preplanned islands might become a hedge against cascading failures and uncontrolled separation.

In practice, preplanned islanding will be practical only if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for preplanned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands to enable them to function independently of the grid. Moreover, standing up islands would severely disrupt day-to-day service for noncritical customers and create instabilities for surrounding systems that could produce additional service disruptions. Accordingly, preplanned islanding might be considered a “huge-regrets” emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created.

DOE and its industry partners should also consider developing preattack emergency orders that fall between the two extremes of no-regrets options and highly disruptive measures. For example, to avoid remote execution of destructive malware on utility networks, orders might direct utilities to disconnect their systems from the internet. Utilities could also take additional measures to isolate or compartmentalize all control systems. Implementing these

measures would curtail potential attack vectors, but would do so at a price. Disconnecting from the internet would hobble wholesale market operations, disable email as a basic communications tool, affect an entity’s access to other means of communications (i.e., E-ISAC and DOE portals), impact an entity’s ability to comply with regulatory requirements, and produce other undesirable consequences. Any unexpected challenges in isolating or compartmentalizing the control systems that are critical to the functioning of the grid could also jeopardize normal service. Nevertheless, if industry and its government partners can preplan to anticipate and overcome these challenges, even highly disruptive preattack options may be useful to protect the grid from cascading failures.

## Extraordinary Measures when Attacks Are Occurring

Emergency orders when attacks are underway can help utilities prevent widespread instabilities, cascading failures, and uncontrolled separation. Under the auspices of the ESCC, utilities and their resilience partners are already developing “extraordinary measures” to operate the grid if adversaries disable or corrupt SCADA (supervisory control and data acquisition) systems, state estimators, and other operational technology hardware and software components on which utilities typically rely.<sup>133</sup> For example, the North American Transmission Forum is leading an initiative on supplemental operating strategies to help power companies manually cope with the loss of energy management systems and/or SCADA across a large geographic footprint.<sup>134</sup>

---

<sup>133</sup> These extraordinary measures include resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary backup systems, and development of supplemental operating strategies use in “degraded states.” See “ESCC: Electricity Subsector Coordinating Council,” ESCC.

<sup>134</sup> Galloway, “Advancing Reliability and Resilience of the Grid,” 2.



These industry efforts provide a basis to develop grid security emergency orders for extraordinary measures when attacks are under way. So, too, do existing BPS emergency operating plans, capabilities, and operational requirements to manage the grid instabilities. Options for such orders vary in terms of the disruption they would inflict on normal grid operations.

Figure 5 provides an example of a low-disruption order for this phase: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate needs or for the next day). These entities have taken extensive measures to keep market functions separate from their operational control of the grid. Many entities also have mechanisms in place to operate when markets are temporarily suspended. Over extended periods, however, cyber attacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, undercut the valuation of power companies on Wall Street, and magnify the damage to the US economy that attacks on the grid will create.

Regional transmission organizations are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the transmission operator<sup>135</sup> for the Mid-Atlantic and other US regions, has called for the development of mechanisms to permit “nonmarket” operations in extreme circumstances.<sup>136</sup> A number of options exist to provide for such operations. For example, if the secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell

power at a fixed price predetermined by DOE.<sup>137</sup> Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high-benefit/low-disruption emergency orders, including orders for maximum power generation when attacks are under way, will also fall into this category.<sup>138</sup>

Industry and government partners will also need to develop more disruptive emergency orders that can protect grid reliability in extraordinary circumstances. One option to do so involves operating an area in a generation-deficient state for a prolonged period, supported (when practical) by power imported from neighboring regions. The top center box of Figure 5 provides another prominent example: prioritized manual load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by selectively shedding load and implementing rotating blackouts.<sup>139</sup>

A failure to shed load contributed to the cascading failures in the major 2003 blackout. After-action reports from that event found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission

<sup>135</sup> The NERC glossary defines *transmission operator* as “the entity responsible for the reliability of its ‘local’ transmission system, and that operates or directs the operations of the transmission Facilities.” *Transmission operator area* is defined as “the collection of Transmission assets over which the Transmission Operator is responsible for operating.” See NERC, *Glossary*.

<sup>136</sup> PJM, “Comments and Responses,” 6, 39–40.

<sup>137</sup> Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. PJM, “Comments and Responses,” 39.

<sup>138</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual 13*, 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see MISO, “MISO January 17–18 Maximum Generation Event Overview.”

<sup>139</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 11.

lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. A US–Canada task force found that “timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio.”<sup>140</sup> In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.<sup>141</sup>

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for transmission operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation for building emergency orders to reduce the risk that physical and cyber attacks will create cascading blackouts.

One way to shed load would be to order power companies to execute rotating blackouts. In such controlled outages, grid operators interrupt service on a rotating basis to sequential sets of distribution feeders for limited periods (typically twenty to thirty minutes).<sup>142</sup> Grid operators employed rotating blackouts to help protect grid reliability during the “Big Chill” that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT’s rotating blackouts during the event affected a total of 4.4 million customers.<sup>143</sup> The temporary blackouts were no doubt disruptive. However, by reducing the risk of cascading failures, those

outages offered compelling system-wide benefits for protecting reliability.

But rotating blackouts will not offer the best option for load shedding in all grid security emergencies. In the event of a massively disruptive attack, an emergency order might require utilities to shed load without implementing rotating blackouts, because such rotating outages could introduce unacceptable reliability risks during a chaotic and rapidly changing situation. As an alternative, utilities can implement “brownouts”: that is, conduct voltage reductions to maintain a continual balance between supply and demand within a balancing area.<sup>144</sup> However, brownouts and rotating blackouts share a serious limitation: they affect all customers equally. But not all customers will be equally important in a grid security emergency. DOE and industry will need orders and implementation plans for manual, prioritized load shedding, so utilities can focus on sustaining power flows to hospitals and other critical loads while also reducing the risk of cascading power failures. NERC already requires BPS entities to have plans for both automatic and manual load shedding.<sup>145</sup> Utilities and DOE should use these requirements as the starting point to design emergency orders for extraordinary measures that would supplement what BPS entities are already prepared to do to if major instabilities occur.

## Emergency Orders to Support Power Restoration

The rightmost column in Figure 5 provides the third category for emergency orders: those that can help grid owners and operators restore power after widespread

<sup>140</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 147.

<sup>141</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 77.

<sup>142</sup> NERC, *Reliability Terminology*, 1.

<sup>143</sup> FERC and NERC, *Restoration and Recovery Plans*, 61.

<sup>144</sup> NERC, *Reliability Terminology*.

<sup>145</sup> NERC standards currently emphasize automatic load shedding to protect grid reliability. See NERC, *Standard PRC-006-3*; and NERC, *PRC-010-2*. However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing emergency orders to prevent or mitigate cascading failures. See NERC, *EOP-011-1*.

outages occur. In past cascading failures of the US electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days (and in some cases much less time) because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators, transmission lines, and other system components are designed to trip offline when instabilities occur, thereby protecting them from damaging power surges—and leaving them available to help rapidly reestablish the flow of power.<sup>146</sup> However, if cyber or physical attacks destroy critical system components, requirements to repair or replace such assets could greatly lengthen and complicate the restoration of service. Emergency orders can support restoration operations and better align them with national-level priorities.

Emergency orders for the restoration phase can also account for the risk that adversaries may continue their attacks as power companies begin to restore service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to US military bases and other vital facilities and to seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeting power restoration operations can help adversaries achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply. Risks of reattack should help drive the design of restoration-phase emergency orders.

Advanced persistent threats hidden in utility networks will pose especially significant challenges for restoration. This malware may enable adversaries to conduct recurring attacks based on timing or network

conditions. Unless utilities thoroughly eradicate such malware, repeated outages could impede restoration operations and put the grid at sustained risk of cascading failures.<sup>147</sup> Physical attacks against restoration personnel and replacement equipment in transit would pose additional problems. Grid security emergency orders can help utilities restore electric service even if they remain “under fire” from cyber and kinetic weapons.

Such orders will differ in the degree to which they could alter existing utility plans to restore power. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks, and barges) from where power companies store them to where they are needed as replacements.<sup>148</sup> Subsequent portions of this report examine how DOE could collaborate with other federal agencies and state and local officials to waive transportation regulations and bolster security support for such operations. The secretary could also issue orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, ports, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these prioritized customers. Emergency orders can help incorporate other national security-related assets that utility plans do not typically include, such as components of the defense industrial base essential for resupplying US forces abroad.

DOE and its industry partners should also create template emergency orders for in extremis restoration operations that would more sharply depart from existing industry plans and procedures. The upper right-hand box of Figure 5 offers an example

---

<sup>146</sup> NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, 1.

<sup>147</sup> Homeland Security Advisory Council, *Final Report*, 7.

<sup>148</sup> DOE, *Strategic Transformer Reserve*, 12–13.

of one such option. If adversaries damage or destroy an extraordinarily large number of transformers, the secretary might order utilities to remove surviving in-service transformers in the same voltage class from their substation and transport them to serve vital national security facilities in the National Capital Region or other areas. Orders of this kind could create severe disruptions in existing service. They might even impede system restoration if utilities and their government partners have not adequately prepared to account for challenges regarding transformers' technical specifications and the BPS's overall configuration. However, if these challenges can be addressed, the benefits might be greater still for helping the United States defeat its adversaries.

Other in extremis orders could help utilities operate the grid if equipment damage is so extensive (or reattacks are so effective) that full system restoration will require many weeks or even months. The FERC/NERC study on severe impact resilience (May 2012) found that coordinated cyber and physical attacks may force the grid into a "new normal" state of "degraded planning and operating conditions" that could last for months or years, including reduced generation and transmission resources and planned and unplanned rotating blackouts.<sup>149</sup> DOE and power companies should consider how emergency orders and supporting regulatory waivers might help electric utilities serve priority loads and accelerate restoration under new normal conditions.

One option to do so is to preplan for the waiver of selected reliability standards. The *Severe Impact Resilience* study recognized that catastrophic events could "put entities in a position where they cannot comply with all standards." However, in part due to the difficulty of predicting the circumstances that entities will face, the study recommended against preplanning for waivers. Instead, the study proposed relying on entities to "do the right thing" for reliability

and public safety" and self-report violations as circumstances permit.<sup>150</sup>

NERC should reconsider this conclusion in light of the secretary's new grid security emergency authorities and the waiver provisions they entail. FERC, NERC, and their industry and government partners should identify specific regulatory waivers and related measures that could provide the basis for utilities' contingency planning for new normal operations.

One such option lies in reliability standards for managing unforeseen contingencies. Currently, NERC standards require BPS entities to operate in an N-1 state: that is, they must be able to sustain service even if they suffer the most severe single contingency (such as the loss of a single critical line, transformer, or generator) possible in their system.<sup>151</sup> Operators may be required to shed load prior to any contingency to maintain the N-1 state. These requirements apply during normal day-to-day operations as well as during system restoration.

Returning to an N-1 state in the face of coordinated cyber and physical attacks is likely to be a lengthy process involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. To help enable utilities to serve critical facilities during such sustained events, the secretary might issue emergency orders that explicitly allow utilities to function in an N-0 operating state (as long as doing so did not risk causing cascading failures or equipment damage).<sup>152</sup>

Issuing such orders could entail important benefits. Operating at N-0 would give utilities greater operating flexibility and ensure that entities can continue to serve as much load as possible during a grid security

<sup>149</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

<sup>150</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 17.

<sup>151</sup> NERC, *BAL-002-2(i)*, requirement R2; NERC, *TOP-001-3*, R12 and R14; and NERC, *IRO-008-2*, R5 and R6.

<sup>152</sup> For N-0, all elements must be within thermal and voltage limits prior to any contingency.



emergency, including military installations and other priority customers. Unlike under N-1 operations, entities would be required to shed load only prior to any contingency for the most severe single contingencies if any of those single contingencies would cause cascading failures, or after a contingency that required load shedding to eliminate overloads or low voltage.

But operating at N-0 would also entail significant risks. N-1 standards exist for compelling reasons: they help protect grid reliability against severe contingencies. Deviating from N-1 requirements will create greater risks of causing further blackouts in new normal conditions. Moreover, N-0 operations would require even greater coordination among BPS entities (including reliability coordinators, transmission owners, and local control centers), as a single outage could result in equipment overloads or voltage violations and require extraordinary mitigation measures. Accordingly, this option will be feasible only if DOE partners with FERC, NERC, and entities to fully understand and mitigate such risks, as well as maximize the potential benefits of N-0 operations for serving critical national security-related loads.

## Additional Emergency Order Design Parameters and Supporting Initiatives

Adversaries will attempt to black out the US grid to achieve their broader political, economic, and military objectives in a conflict. Government agencies and the electricity subsector should design emergency orders to help prevent attackers from accomplishing their objectives, and—ideally—to help deter them from attacking at all.

However, deterring and defeating attacks on the grid will require resilience improvements beyond the electricity subsector. Attackers may simultaneously strike electric and communications systems to both disrupt the grid and impede the issuance and

implementation of emergency orders. Adversaries may also seek to incite public panic through social media and other information warfare operations to advance their broader political objectives. Countering such efforts will require unprecedented collaboration among utilities, government agencies, media, and the broader telecommunications sector.

Designing and implementing emergency orders to blunt attacks by Russia, China, and other potential high-capability adversaries will place extraordinary burdens on electric utilities—burdens that few ratepayers and utility investors will be eager to bear on their own. To help power companies meet these challenges, it will be essential to fully leverage the regulatory waiver and cost-recovery provisions of the FPA, and examine whether Congress should expand these provisions as threats continue to intensify.

## Deterring and Defeating US Adversaries

The US *National Security Strategy* emphasizes that cyber threats to US critical infrastructure are becoming increasingly severe. In particular, the strategy notes that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>153</sup> Pairing cyber attacks with coordinated physical strikes against transformers and other critical grid infrastructure would exacerbate these disruptive effects.

The strategy identifies two primary means for deterring catastrophic attacks, both of which can be supported by emergency orders and implementation plans:

- (1) Convince adversaries that they will suffer “swift and costly consequences” if they strike the grid or other US targets, and that the United States “can and will defeat them” if deterrence fails.<sup>154</sup>

<sup>153</sup> White House, *National Security Strategy*, 13, 28.

<sup>154</sup> White House, *National Security Strategy*, 28.



- (2) Strengthen infrastructure resilience to create “doubt in our adversaries that they can achieve their objectives” if they do attack (i.e., deterrence by denial).<sup>155</sup>

### **Deterrence through Cost Imposition: Protecting Defense Critical Electric Infrastructure**

In amending the FPA, Congress placed a particular emphasis on the need to protect the reliability of defense critical electric infrastructure (i.e., grid components that serve military bases and other facilities “critical to the defense of the United States” and vulnerable to the disruption of grid-provided electricity).<sup>156</sup> Emergency orders to protect such infrastructure can help ensure that US bases have the power they need to respond to attackers. But prioritizing defense installations for support in grid security emergencies will require deeper analysis of US deterrence requirements, given DOD’s growing dependence on civilian assets and functions to execute defense missions. Deterrence by cost imposition will also depend on convincing potential adversaries that the United States will be able to identify them as the perpetrators of attacks on the grid. DOE and its industry partners should explore how emergency orders can facilitate attack attribution, as well as provide broader support for the credibility of the US deterrence posture.

A relatively small number of military bases are responsible for inflicting unacceptable costs on potential adversaries. The US Defense Science

Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of US strike systems (cyber, nuclear, and nonnuclear) and supporting infrastructure to ensure “that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks.”<sup>157</sup> Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which US strike systems rely and ensure that they have reliable power even in extended conflicts.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The strategy emphasizes that “we must convince adversaries that we can and will defeat them—not just punish them if they attack the United States.”<sup>158</sup> Defeating adversaries in regional contingencies in the South China Sea, the Baltics, or other potential conflict zones will place special burdens on US grid resilience. US capabilities to conduct operations abroad are increasingly dependent on domestic military and civilian assets. In particular, a vast array of US defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy, operate, and sustain US power projection forces for regional conflicts.

This dependence makes the grid a prime target for attack. The DOD *Mission Assurance Strategy* notes that adversaries may seek to disrupt power projection capabilities by attacking the domestic infrastructure systems on which they depend. In particular, the strategy warns that “potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting

<sup>155</sup> White House, *National Security Strategy*, 13, 28. The literature on security studies defines deterrence by denial in a variety of ways. This report follows the definition used in the *National Security Strategy*, which is consistent with the definition employed in the Obama administration’s deterrence policies. See Lynn, “Defending a New Domain.” For broader studies of deterrence by denial, and critiques of the way in which the strategy employs the term, see Fischerkeller and Harknett, “Deterrence Is Not a Credible Strategy”; Mitchell, “Case for Deterrence by Denial”; Gerson, “Conventional Deterrence,” 40; and Nye, “Deterrence and Dissuasion,” 56–58.

<sup>156</sup> 16 U.S.C. § 824o–1, (a)(4).

<sup>157</sup> Miller and Gosler, “Memorandum.” See also pp. 3, 6–7, 11–12, and 17–18 of the report.

<sup>158</sup> White House, *National Security Strategy*, 28.

critical defense and supporting civilian capabilities and assets,” including the US power grid.<sup>159</sup>

Ensuring the availability of resilient power for ports and other civilian assets essential for power projection will require emergency orders to serve an expanded set of customers, far beyond those responsible for strike operations. These orders will also need to encompass a much larger array of defense critical electric infrastructure owners and operators.

Electric companies and defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds from separate high-voltage transmission substations to serve defense installations provides a valuable means of strengthening resilience against physical attacks.<sup>160</sup> Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.<sup>161</sup> Utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as power islands independent of the surrounding grid.<sup>162</sup>

While valuable, these initiatives do not eliminate the need to develop national defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases and will not necessarily provide resilience against cyber attacks (since even redundant feeds may share common cyber vulnerabilities). Emergency generators will break down in long-duration outages. Moreover, resupplying them with fuel will become increasingly difficult at installations that lack massive storage

tanks. Large-scale microgrids for islanded operations can provide more resilient power. DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction and scale them to serve infrastructure loads outside the base that are essential for on-base operations. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for war fighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, including the intermodal transportation systems that help deploy and sustain US forces abroad.

DOE and its industry partners can design emergency orders to support US deterrence credibility and power projection capabilities far more quickly and with less infrastructure investment. However, for utilities to implement these orders, they must first know which customers are of the highest priority for sustaining and restoring service when enemies strike. Section 215A of the FPA provides the ideal starting point develop and share such data. The act requires the secretary of energy, in consultation with other federal agencies and grid owners and operators, to identify and designate “critical defense facilities” in the forty-eight contiguous states and the District of Columbia that are “(1) critical to the defense of the United States; and (2) vulnerable to a disruption of electric energy provided to such facility by an external provider.”<sup>163</sup> Congress’s definition of defense critical electric infrastructure also helps guide implementation of that requirement. Such assets include “any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]” as a critical defense facility, “but is not owned or operated by the owner or operator of such facility.”<sup>164</sup>

<sup>159</sup> DOD, *Mission Assurance Strategy*, 1.

<sup>160</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39.

<sup>161</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 40.

<sup>162</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39. See also Van Broekhoven et al., *Microgrid Study*; and Marqusee, Schultz, and Robyn, *Power Begins at Home*, 13–15. A number of “islandable” microgrid projects are under way at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See McGhee, “EEI Executive Advisory Committee,” 4; and Kaften, “DoD Tests Energy Continuity.”

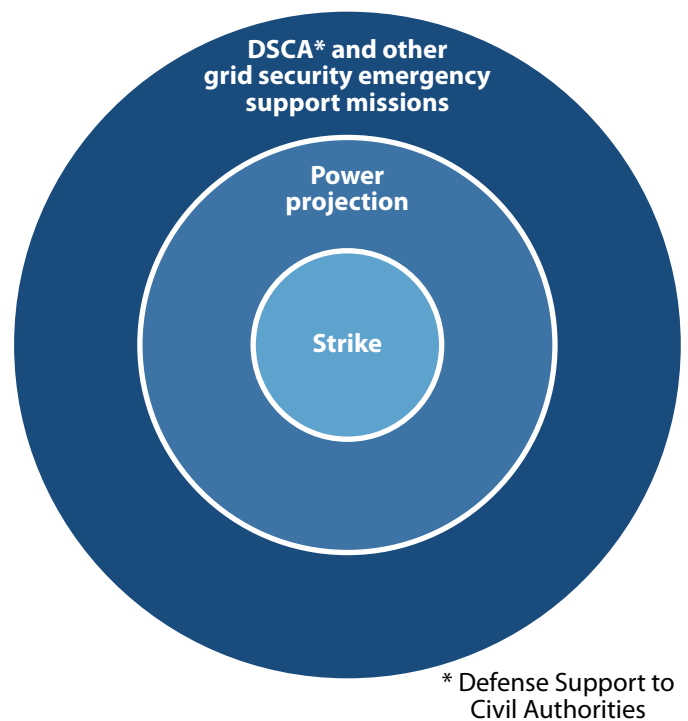
<sup>163</sup> 16 U.S.C. § 824o–1, (c).

<sup>164</sup> 16 U.S.C. § 824o–1, (a)(4).

DOE is already working with DOD to identify defense critical electric infrastructure and the installations this infrastructure serves. DOD has a well-established, continuously updated list of critical military bases and other DOD assets to support this identification process.<sup>165</sup> However, deterrence and power projection will also depend on sustaining electric service to a diverse array of ports, transportation systems, and other civilian-owned infrastructure. Figure 6 illustrates how DOE, DOD, and their partners might categorize all such defense-related assets and the defense critical electric infrastructure that grid security emergency orders should help protect.

At the innermost core lie those installations and supporting infrastructure capable of inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital. Protecting the reliability of the defense critical electric infrastructure on which they depend should be the top nationwide priority for developing emergency orders and company-specific implementation plans.

The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining these assets abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the US grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. DOD is in the process of identifying the specific facilities and supporting infrastructure that are required to help execute operational plans around the globe.<sup>166</sup> The department also has well-established criteria and assessment methods to prioritize these supporting assets for risk mitigation.<sup>167</sup> DOD and DOE should use these tools to identify the broader set of defense critical electric infrastructure needed for deterrence



**Figure 6. Categories for Protecting Defense Critical Electric Infrastructure**

and to help power companies preplan to support critical assets within their service footprints.

The third circle includes the still larger array of defense installations, including National Guard bases, which would be essential for providing defense support to civil authorities if disruptions of the grid jeopardize public health and safety.<sup>168</sup> During Hurricane Maria (2017), Superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, lodging, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and delivering other assistance. Protecting or rapidly restoring the reliability of the defense critical electric infrastructure that supports

<sup>165</sup> See DOD, *Manual 3020.45*; and DOD, *Directive 3020.40*.

<sup>166</sup> DOD, *Directive 3020.40*.

<sup>167</sup> DOD, *Manual 3020.45*.

<sup>168</sup> Of course, many National Guard installations that could conduct defense support operations may also be responsible for assisting war fighting operations abroad, and would therefore fall within the second circle as well.

these defense-support-to-civil-authorities functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public.<sup>169</sup>

Building preparedness for grid security emergencies can also help meet an underlying challenge for deterrence: attack attribution. To convince foreign leaders that they will suffer swift and costly consequences if they strike the grid, those leaders must first believe that the United States will be able to identify them as the attackers.<sup>170</sup> The Federal Bureau of Investigation (FBI) and other federal agencies are improving their attribution capabilities.<sup>171</sup> US agencies also devote massive resources to human and technical intelligence collection on potential adversaries, which could further assist attack attribution.<sup>172</sup> Nevertheless, adversaries may seek to strike in ways that complicate attack forensics by employing wiper tools and using other tactics, techniques, and procedures to cover their tracks.<sup>173</sup>

Emergency orders can help defeat adversaries' efforts to evade attribution. By refining the FPA's information sharing mechanisms and building them into emergency orders, utilities and their government partners can strengthen their ability to share malware samples and other information on threat signatures.<sup>174</sup> New technologies can bolster such collaboration. For

example, the Containerized Application Security for Industrial Control Systems project is designed to help grid operators isolate and capture malware on their systems, enabling samples to be shared with government agencies while still preventing that malware from disrupting system operations.<sup>175</sup>

Developing emergency orders and implementation plans to defend the grid can also provide broader support for attribution. James Miller notes that "while cyber hardening of US critical infrastructure will never be good enough to prevent a Russia or China from being able to threaten a major attack, it can cause them to have to be 'noisier' to do so, thereby boosting our confidence in attribution."<sup>176</sup> Emergency measures to protect grid reliability can complicate attack planning and, ideally, drive adversaries to strike in ways that will make them easier to identify.

### **Deterrence by Denial: Protecting Critical Electric Infrastructure**

Convincing adversaries that they will suffer unacceptable costs if they strike the grid is only one means of deterring such attacks. Another means is to reduce the benefits that adversaries expect to achieve by attacking. In classical deterrence theory, both factors combine to influence an adversary's decision on whether to strike. As Joseph Nye Jr. puts it, "deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."<sup>177</sup>

The *National Security Strategy* calls for measures that can prevent attackers from achieving the goals they seek and thereby strengthen deterrence by denial. The strategy states that "we must ensure the ability to deter enemies by denial, convincing them that they cannot accomplish their objectives through the use of

<sup>169</sup> Countering such adversary efforts will also require protecting electric service to financial institutions, regional hospitals, and other civilian assets essential to the US economy and public health and safety. The next section of the report examines these requirements and their implications for deterrence and emergency order design.

<sup>170</sup> On the tasks that attribution comprises, see Lin, "Escalation Dynamics," 49–50.

<sup>171</sup> Smith, "Roles and Responsibilities." See also Newman, "Hacker Lexicon."

<sup>172</sup> Miller, "Cyber Deterrence."

<sup>173</sup> Newman, "Hacker Lexicon."

<sup>174</sup> See 16 U.S.C. § 824a–1, (d). Later sections of this report provide a more detailed assessment of provisions for improved information sharing.

<sup>175</sup> "Sandia's Grid Modernization Program Newsletter," Sandia National Laboratories.

<sup>176</sup> Miller, "Cyber Deterrence."

<sup>177</sup> Nye, "Deterrence and Dissuasion," 45.



force or other forms of aggression.”<sup>178</sup> Ensuring that the grid and other infrastructure sectors can survive attacks and rapidly recover from service interruptions plays an especially important role in the administration’s deterrence posture. The strategy notes that “a stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.”<sup>179</sup> More recent statements of administration policy also note that deterrence by denial “must be foundational to the U.S. deterrence approach,” and that US efforts must continue “to deny adversaries the benefits of their malicious cyber activities.”<sup>180</sup>

Emergency orders and implementation plans may be able reduce the benefits that adversaries expect to achieve by attacking the grid. Preattack orders to bolster grid defenses can impede adversary efforts to disrupt grid reliability. Once attacks are under way, orders for prioritized load shedding and other extraordinary measures can help limit the damage the adversaries may hope to inflict on financial institutions, hospitals, and other electricity-dependent facilities. Orders that accelerate power restoration to these critical facilities may also reduce the effects of an attack, and thereby strengthen deterrence by denial.

The FPA is ready-made to support such improvements. In addition to protecting defense critical electric infrastructure, and thereby assisting deterrence through cost imposition, the act also authorizes orders to protect a much broader portion of the grid: critical electric infrastructure. Such infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>181</sup> Orders to help utilities defend critical electric infrastructure can reinforce deterrence by denial—and, if deter-

rence fails, reduce the devastation that adversaries will create.

However, developing and implementing such orders will entail major challenges. Some deterrence theorists doubt whether deterrence by denial is practical in cyberspace, in part because offensive capabilities are so much stronger than cyber defenses. The conclusion of this report will examine those arguments and explore broader opportunities to bolster deterrence and help the United States defeat our adversaries if conflicts nevertheless occur. First, however, DOE and its partners will need to overcome two impediments to protecting critical electric infrastructure: determining which specific facilities and functions are truly critical, and securely sharing that information with utilities so they can refine their operational plans for grid security emergencies.

### **Building a “Section 9+ List:” Prioritizing Infrastructure for Sustainment and Restoration**

Identifying and prioritizing critical electric infrastructure will be far more difficult than doing so for defense critical electric infrastructure. If adversaries create cascading blackouts across one or more interconnections, the disruption of many thousands of civilian-owned facilities could negatively affect national security, the US economy, and public health and safety. Utilities cannot possibly prioritize the flow of power to all such facilities. Government agencies and their private sector partners will need to determine which specific customers (and the critical electric infrastructure that serves them) are most vital to the nation and must continue to receive power if widespread instabilities occur.

Executive Order 13636 (February 2013) provides an existing methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the secretary of homeland security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security,

<sup>178</sup> White House, *National Security Strategy*, 28.

<sup>179</sup> White House, *National Security Strategy*, 13.

<sup>180</sup> DOS, *Recommendations*, 2.

<sup>181</sup> 16 U.S.C. § 824o–1, (a)(2).



or national security.”<sup>182</sup> That standard—catastrophic damage—provides a useful criterion to identify the highest-priority assets and associated critical electric infrastructure for protection by emergency orders in grid security emergencies. Over time, orders and contingency plans could gradually encompass less-critical facilities and grid infrastructure.

Of course, the section 9 methodology and subsequent list were never intended to support the implementation of section 215A of the FPA. As a result, the section 9 methodology falls short of meeting all the requirements for supporting emergency order design. One gap lies in the threats that drive the selection of critical assets. Section 9 focuses exclusively on infrastructure at risk from cyber attacks. The FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on electric systems. Executive Order 13636’s section 9 requirements also create a “corporate”-level list that is not broken down into the key assets within those corporations (i.e., facilities, systems, and nodes). More fine-grained data and analysis will be required to identify facilities for which sustained electric service will be most crucial. Efforts to prioritize grid service will also need to account for the increasingly complex interdependencies between US infrastructure sectors.<sup>183</sup>

Despite these shortfalls, Executive Order 13636’s methodology can provide a valuable starting point for identifying the most vital critical electric infrastructure and supporting assets. DOE and its industry partners should leverage that methodology to create a “section 9+” list, tailored to fulfill FPA emergency order requirements. Other government initiatives to prioritize critical infrastructure could

also make valuable contributions to the list and overall prioritization effort. For example, DHS’s May 2018 cyber strategy emphasizes the importance of “identifying the most critical [federal] systems and prioritizing protections around those systems.”<sup>184</sup> A number of other initiatives could provide significant value as well.<sup>185</sup> Building a section 9+ list would also benefit from the inclusion of input from cleared state regulators and homeland security and emergency management officials.

DHS’s National Risk Management Center can help integrate these sources of data and develop a comprehensive, cross-sector basis for prioritizing the sustainment and restoration of power to critical facilities. Government agencies within the center will collaborate with the private sector to “identify, assess, and prioritize efforts to reduce risks to national critical functions, which enable national and economic security.” One immediate task will be to “help define what is truly critical.”<sup>186</sup> As this work

<sup>184</sup> DHS, *Cybersecurity Strategy*, 8.

<sup>185</sup> There are numerous programs that DOE and its partners could leverage to build the section 9+ list. DHS’s National Critical Infrastructure Prioritization Program aims to identify “nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance.” See DHS, *NIPP 2013*, 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on “lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity” (p. 24). Despite its focus on terrorist threats, *Homeland Security Presidential Directive 7* also requires the secretary of homeland security to identify and prioritize systems and assets that, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the “loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States” and lower jurisdictions. The national-level priorities on this list could also be helpful. 6 U.S.C. § 124l, (a)(2).

<sup>186</sup> “National Risk Management Center Fact Sheet,” DHS.

<sup>182</sup> Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*.

<sup>183</sup> For methodologies and data-gathering strategies to assess cross-sector interdependencies, see EIS Council, *E-PRO Handbook III*; and Homeland Security Advisory Council, *Final Report*.

goes forward, the center's efforts could contribute to the development of a section 9+ list that will be essential for grid security emergency preparedness.

### **Sharing the Section 9+ List and Protecting Critical Electric Infrastructure Information**

In addition to identifying assets most in need of power, it will also be essential to share that data with the utilities responsible for providing prioritized service. Current section 9 guidance lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the federal government tells grid owners and operators if they are on the section 9 list, it rarely informs them about the section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own system configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data with government partners. Public sector leaders will need to reinforce their industry counterparts' confidence that government agencies will not use company-provided information for regulatory compliance, antitrust, or other purposes not explicitly approved through industry-government dialogue.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that critical companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations or supply chains in one industry can produce unintended and unforeseen effects on overall system resilience. Private

companies will need to help government agencies modify the section 9+ list as they reconfigure their operations and create new dependencies on outside service and product providers.

Securing and limiting the distribution of this classified data will also be a prerequisite for countering potential attacks. If adversaries acquired the section 9+ list, it would provide a roadmap that they could use to maximize their devastation of US critical infrastructure. However, measures to protect this data must be complemented by improved mechanisms to provide sensitive information to industry personnel who have the requisite security clearances.

Section 215A of the FPA offers a starting point to meet these requirements. The FPA provides for the sharing of critical electric infrastructure information, defined as information generated by FERC or other federal agencies related to identified (or proposed) critical electric infrastructure "that is designated as critical electric infrastructure information by the Commission or the Secretary" or that qualifies under FERC's critical energy infrastructure information scheme.<sup>187</sup> The FAST Act amendments directed FERC to facilitate the voluntary sharing of such information "with, between, and by" BPS entities and their government partners.<sup>188</sup> The amendments also require FERC to create criteria and procedures to designate certain information as critical and prohibit unauthorized disclosure of that information.<sup>189</sup> To help meet these requirements, FERC incorporated and is building on its well-established mechanisms to protect critical energy infrastructure information.<sup>190</sup>

<sup>187</sup> The definition excludes classified national security information. 16 U.S.C. § 824o-1, (a)(3).

<sup>188</sup> This includes NERC, the E-ISAC, regional entities, and "other entities determined appropriate by the Commission." See 16 U.S.C. § 824o-1, (d)(2)(D).

<sup>189</sup> 16 U.S.C. § 824o-1, (d)(2).

<sup>190</sup> FERC, *Regulations Implementing FAST Act Section 61003* (Order No. 833), 157 FERC ¶ 61,123, 13. See also FERC,

Other initiatives are also under way to provide for the protected data sharing essential for preplanning grid security emergency operations. DOE is working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate assets identified as defense critical electric infrastructure. Going forward, DOE, FERC, and their industry partners should refine their equivalent mechanisms to securely distribute data on critical electric infrastructure and the water systems, communications centers, and other essential non-defense assets that must continue to function in grid security emergencies.

## Communications Requirements for Issuing and Employing Emergency Orders

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phones and other normal means of communication fail. These systems often provide connectivity with neighboring BPS entities and, to an increasing extent, entities that are farther away. Under the ESCC, industry has also built an extensive set of playbooks to help companies decide what to tell customers about an incident and to unify messaging between government officials and industry representatives on estimated times of restoration and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. Preparedness for grid security emergencies will require additional progress in four areas: (1) refining consultative mechanisms and protocols for the sequential (though potentially overlapping) phases of such emergencies; (2) ensuring that communications

systems can survive adversaries' attacks; (3) authenticating emergency orders and protecting the security of sensitive data; and (4) determining what to say to the US public and accounting for the risk that adversaries will conduct information warfare operations to intensify panic and incite disorder.

## Initial Consultations and Sustained Communications

As with the phases of grid security emergency declarations, the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Preattack consultations constitute the initial stage. As noted above, the FPA specifies that before the secretary issues emergency orders, DOE will consult with power companies and other BPS stakeholders "to the extent practicable . . . regarding implementation of such emergency measures."<sup>191</sup> This report recommends that federal officials also consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The grid security emergency rule clarifies how DOE's Office of Electricity Delivery and Energy Reliability will consult on emergency orders.<sup>192</sup> The rule states that, if practicable, the E-ISAC is one of the organizations the secretary will consult. Such consultations will be particularly useful for sharing data (including classified data) on attacks that are imminent or under way. The rule also notes that DOE will consult with the ESCC. The ESCC will provide an especially valuable source of industry perspectives on grid security emergency declarations and emergency orders because it represents all components of the electricity subsector and has extensive experience in coordinating the industry's incident response operations. In addition, the rule states that "efforts

*Regulations Implementing FAST Act Section 61003* (Order No. 833-A), 163 FERC ¶ 61,125; and 18 CFR 388.113.

<sup>191</sup> DOE, "RIN 1901-AB40," 1774.

<sup>192</sup> DOE, "RIN 1901-AB40," 1181.

will be made” to consult with NERC, regional entities, “owners, users, or operators” of critical and defense critical electric infrastructure (including regional transmission operators), appropriate federal and state agencies, and other grid reliability stakeholders.

Issuing emergency orders constitutes the second stage. DOE’s grid security emergency rule states that the department will “communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances.”<sup>193</sup> The E-ISAC will likely play a critical role in such communications, since it maintains a detailed, continuously updated list of all BPS owners, operators, and registered users (distribution entities). DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.<sup>194</sup> As long as these mechanisms can be hardened as necessary to survive adversaries’ attacks, leveraging them for grid security emergencies will be much more efficient than creating a separate, unfamiliar system for communicating emergency orders.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders. Attacks on the grid are unlikely to be “one and done.” As adversaries continue to try to destabilize the grid, and power companies respond with emergency operations to protect and restore electric system reliability, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional orders and response activities—potentially on a nationwide basis.

Reliability coordinators will be a critical touchpoint between DOE and individual BPS entities, serving as a focal point between DOE (and other government

leaders) and the power companies that are in their purview. This positioning makes them well suited to communicate secretary-issued orders to individual utilities. Moreover, given reliability coordinators’ responsibilities and authorities to help maintain grid reliability when incidents occur, they will also be ideally positioned to understand how grid security emergency orders should supplement BPS emergency operations that are already under way.

Sustained communications will also be necessary to meet an additional FPA requirement: responding to DOE requests for information on the implementation of emergency orders. The grid security emergency rule specifies that “beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order.”<sup>195</sup> Sustained communications links between DOE and BPS entities will be required to meet such requests for information. However, beyond compliance issues, continuous communications will also be required as government and industry partners assess the effectiveness of emergency operations and identify requirements for additional actions.

### Survivability of Communications

Adversaries will have compelling incentives to combine attacks on the grid with strikes against US communications systems. The 2015 attack on Ukraine’s electric grid illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone networks; the latter attack prevented customers from reporting outages and disrupted grid operators’ ability to conduct restoration operations.<sup>196</sup> In turn, if adversaries can lengthen power outages by disrupting communications systems essential

<sup>193</sup> DOE, “RIN 1901-AB40,” 1181.

<sup>194</sup> DOE, “RIN 1901-AB40,” 1177.

<sup>195</sup> DOE, “RIN 1901-AB40,” 1182.

<sup>196</sup> “Alert (IR-ALERT-H-16-056-01).”



for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications-system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually reinforcing disruptions in both sectors.

We should assume that adversaries will design their attacks to maximize multisector failures, especially since they would already be facing the risk of US response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry–government coordination in grid security emergencies. Enemies might strike communications systems to hobble efforts to share preattack threat data and convey emergency orders. Once attacks on the grid were under way, adversaries could also seek to cripple the communications systems needed to coordinate emergency operations and assess requirements for additional measures.

Strengthening the survivability of existing communications links will be essential to manage these risks. To date, ESCC consultation and coordination mechanisms have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to distributed denial-of-service attacks and a range of other increasingly severe threats,<sup>197</sup> as well to the loss of the grid-provided electricity on which many such systems depend (especially in long-duration outages that put emergency power assets at risk).

Adversaries may also seek to disrupt systems essential for information sharing. For example, the Cybersecurity Risk Information Sharing Program and other E-ISAC notification procedures and portals are in place to alert utilities when adversaries

are implanting malware on critical systems.<sup>198</sup> This includes the E-ISAC’s new Critical Broadcast Program, which is intended to operationalize the organization’s information sharing capabilities.<sup>199</sup> The FBI and DHS also issue alerts to the energy sector, as in the case of CrashOverride.<sup>200</sup> However, many of these warning and information sharing mechanisms rely on the internet or other potentially vulnerable systems. Industry and government should explore options to ensure that they can still convey essential data in the face of sophisticated attacks on the communications sector.

In addition, adversaries may seek to disrupt the issuance of emergency orders. DOE’s grid security emergency rule notes that the department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include “essential actions” to protect BPS reliability, which require recipients to respond as defined in the alert.<sup>201</sup> DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across registered entities. NERC already distributes alerts broadly to BPS users, owners, and operators in North America. Hence, the alert system provides DOE with an opportunity for “one-stop shopping” when issuing emergency orders. The secretary could issue an order to NERC for distribution to both regional operating organizations (regional transmission organizations, independent

<sup>197</sup> Banham, “DDoS Attacks.”

<sup>198</sup> “Energy Sector Cybersecurity Preparedness,” DOE; and “Electricity Information Sharing and Analysis Center,” NERC.

<sup>199</sup> The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See Lawrence, de Seibert, and Daigle, “E-ISAC Update.”

<sup>200</sup> “Alert (TA17-163A).”

<sup>201</sup> “About Alerts,” NERC.



system operators, reliability coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is email based.<sup>202</sup> As such, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also includes only those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for implementing emergency orders for prioritized load shedding and other actions to sustain power to critical facilities.

Moreover, while the NERC alert system could provide a means of communications across BPS users, owners, and operators, NERC primarily uses the system to communicate alerts of voluntary actions to be taken by electric industry stakeholders. Using the NERC alert system to instead communicate a mandatory action pursuant to a DOE emergency order would require clear coordination and communication to ensure that the order and associated requirements for action are fully understood. In addition, while the NERC alert system offers a proven means to convey unclassified information, the system may not be well suited to distribute classified data.

To fill these gaps, industry and government partners should consider measures to bolster the NERC alert system or create fallback options for survivable communications. Satellite phones offer a prominent option for operational coordination. These phones are widely deployed both among BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies.

Retired US Air Force General William Shelton, who directed the US Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community."<sup>203</sup>

Accordingly, power companies are ramping up their investments in terrestrial emergency communications systems that are hardened against cyber and physical attacks and can be used to sustain critical grid functions even if satellite phones fail.<sup>204</sup> Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are under way to build dark fiber or other survivable links between BPS entities—much less between those entities and DOE. The National Infrastructure Advisory Council study *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish "separate, secure communications networks specifically designated for the most critical cyber networks, including 'dark fiber' networks for critical control system traffic and reserved spectrum for backup communications during emergencies."<sup>205</sup>

The council's study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. In doing so, DOE should leverage lessons learned from the communications sector and specifically from the National

<sup>202</sup> "About Alerts," NERC.

<sup>203</sup> Shelton, "Threats to Space Assets," 3.

<sup>204</sup> FERC and NERC, *PRASE*, 15.

<sup>205</sup> NIAC, *Securing Cyber Assets*, 7.

Security Telecommunications Advisory Committee, which has extensive experience in building redundant and survivable systems.<sup>206</sup> However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities “can communicate with utility crews working in the field to manually restore power” and conduct other postattack operations.<sup>207</sup> Survivable communications systems must also be able to coordinate emergency operations across the electricity subsector and with supporting government agencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when those orders are needed most.

### Authenticating and Securing Emergency Orders

In addition to disrupting the availability of communications systems, adversaries may also seek to corrupt the content of emergency orders and coordination messages, and gain access to classified US data to help defeat grid protection measures. One near-term requirement will be to ensure that utilities can authenticate the orders they receive from DOE. Power companies will need to be able to verify that an order has actually come from the secretary, and that adversaries have not altered its content. Verifying the authenticity of orders will be especially important if such orders require extraordinary measures that could further disrupt normal service and affect public health and safety.

Existing mechanisms and protocols to ensure the integrity of subsector communications provide an initial basis to meet these challenges. Other government agencies have also developed authentication protocols that could be adapted for use in grid security emergencies. For example, the *DoD Cybersecurity Discipline Implementation Plan* (February 2016) offers detailed guidance to strengthen authentication in the face of adversary

efforts to exploit communications networks and devices.<sup>208</sup>

Adversaries may also seek to gain access to classified or operationally sensitive emergency orders. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as possible, lest those operations create incentives for adversaries to strike before their advanced persistent threats were disabled. When attacks are under way, it could be useful to deny adversaries the knowledge of where and how BPS entities are prioritizing the flow of power to vital military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important, given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The FPA and subsequent grid security emergency rule provide for the sharing of classified information in grid security emergencies. The rule specifies that:

To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.<sup>209</sup>

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program already have mechanisms and protocols for sharing and securing classified threat

<sup>206</sup> “About NSTAC,” DHS.

<sup>207</sup> NIAC, *Securing Cyber Assets*, 7.

<sup>208</sup> DOD, *DoD Cybersecurity Discipline Implementation Plan*.

<sup>209</sup> DOE, “RIN 1901–AB40,” 1182.

data with BPS entities cleared for access to that data.<sup>210</sup> Industry and government partners should consider building on those mechanisms to support the issuance of classified emergency orders. Ongoing progress under the Cybersecurity Risk Information Sharing Program will be valuable as it serves a growing array of utilities, accesses additional sources of data and advanced analytic tools, and continues other improvements.

DOE and its partners in industry and government might consider sharing this classified data in other ways. For example, DHS and other federal partners such as the FBI and the National Guard have secure video teleconference capabilities. However, these are technologically complex and not seamlessly interoperable with industry systems. Moreover, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Section 215A addresses this issue by ordering the secretary to “facilitate and, to the extent practicable, expedite,” the security clearance process for key personnel of any entity subject to emergency orders to enable “optimum communication” of threat information.<sup>211</sup> DOE should accelerate its ongoing efforts to meet this requirement. The section also grants the secretary and other appropriate federal agencies the authority to provide temporary access to classified information regarding grid security emergencies and subsequent orders to key personnel of complying entities.<sup>212</sup>

Yet, even for utilities with cleared personnel on their staffs, an even smaller number possess the sensitive compartmented information facilities or other infrastructure and government approvals to store classified information. To address those limitations, the grid security emergency rule clarifies that the secretary may declassify information critical to the

emergency response.<sup>213</sup> But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of combatant commander operational plans; when emergency orders may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

### Communicating with the American People

Adversaries may attack the grid not only to disrupt national defense and the economy but also to gain political leverage over US leaders by inciting public panic and disorder. A presidential declaration that the grid faces imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the US public.

Preplanning for public messaging to accompany grid security emergency declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Unifying messaging with governors and other elected officials on estimated restoration times already presents significant challenges in such events. However, those difficulties will be dwarfed by the problems that adversaries can create through cyber attacks. Attackers may:

- Use information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety
- Intensify state and local requests for defense support to civil authorities to deal with these

<sup>210</sup> “Energy Sector Cybersecurity Preparedness,” DOE.

<sup>211</sup> 16 U.S.C. § 824o–1, (e).

<sup>212</sup> 16 U.S.C. § 824o–1, (b)(7).

<sup>213</sup> DOE, “RIN 1901–AB40,” 1778.

anticipated effects, and thereby put pressure on US leaders to divert scarce defense assets and resources from other missions

- Disrupt normal means of communication on which the public will rely for information about the event
- Magnify the inherent difficulties of estimating restoration times by employing advanced persistent threats that enable repeated reattacks and disruptions in grid service until eradicated from BPS networks.

DHS's Social Media Working Group for Emergency Services and Disaster Management has offered preliminary recommendations on how to counter disinformation during disaster response operations.<sup>214</sup> In addition, the ESCC and its members are developing playbooks to help meet disinformation challenges and support public messaging in the event of cyber or physical attacks against the grid.<sup>215</sup> Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that presidential grid security emergency declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Preplanning for message coordination with Canada and Mexico could also be helpful and might leverage the FPA's provisions for such multinational consultations concerning the issuance of emergency orders.<sup>216</sup>

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. For example, some orders that will be valuable for protecting grid reliability, including those for prioritized load shedding, could

cut off electricity to many thousands of customers to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

## The Deeper Value Proposition for Emergency Orders: Political Top Cover, Waivers, and Cost Recovery

The grid security emergency provisions of the FPA do not even mention a significant advantage that orders can provide for industry: they can help protect power companies from the political heat that extraordinary grid protection measures will create. The FPA's provisions for regulatory waivers and cost recovery offer more explicit benefits. Yet, given the risks that utilities could incur in conducting emergency operations, and the investments in infrastructure that may be required to facilitate order implementation, Congress and DOE should consider additional measures to help power companies defend the grid and protect national security.

### Facilitating Operations under Extraordinary Political Circumstances

In responding to natural hazards, power companies can fall under intense pressure to serve the priorities of state and local elected officials. In severe weather events, for example, governors have told utilities to delay sending restoration resources to assist neighboring states until service has been restored to *all* customers (i.e., voters) in the governors' own states.

Cyber and physical attacks on the grid could create still more intense political pressure, and complicate utilities' efforts to serve national priorities versus those most urgent to meet state and local needs. Such attacks will occur in the context of broader risks of all-out war and will magnify public fears in ways that hurricanes or other natural hazards cannot—especially if those attacks are accompanied by

<sup>214</sup> Social Media Working Group for Emergency Services and Disaster Management, *Countering False Information*.

<sup>215</sup> ESCC, "ESCC: Electricity Subsector Coordinating Council."

<sup>216</sup> 16 U.S.C. § 824o-1, (b)(3).



information warfare operations to incite public panic. Governors will have powerful incentives to ensure that utilities in their states take care of their own citizens rather than meeting requests for assistance from power companies in other states.

However, from a national security perspective, not all states and customers within them will be of equal importance for protecting defense critical electric infrastructure. Some low-population states served by utilities with only limited resources are the homes of vital military installations. These utilities may need assistance from out-of-state power companies to supplement their own personnel and response capabilities when adversaries strike.

The electric industry's Cyber Mutual Assistance (CMA) Program will be critical for providing such support.<sup>217</sup> DOE is expanding the technical resources and capabilities available to support CMA response operations.<sup>218</sup> Under the national response event initiative, investor-owned utilities (led by the Edison Electric Institute) are also bolstering mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States.<sup>219</sup> All of these initiatives will be vital for responding to grid security emergencies that entail multiregional disruptions of the BPS or degrade critical electric infrastructure that the infrastructure's owners cannot restore on their own.

Yet, the voluntary nature of these mutual assistance systems could present challenges in grid security emergencies. In hurricanes or other natural hazards, governors and utilities can predict whether or not their states are likely to be struck and either husband their resources accordingly or provide them in response to requests for assistance. Cyber and physical attacks by Russia, China, or other potential adversaries are much less predictable. Enemies may

strike one region before moving on to others. Attacks could even occur on a nationwide basis. Accordingly, elected officials may discourage utility leaders from volunteering resources for mutual assistance in neighboring regions, even if their own states have not yet been struck.

Issuing emergency orders can help utilities address these challenges and serve national priorities. Participants in the Cyber Mutual Assistance Program are already taking steps to account for the risk of multiregional attacks. DOE and its industry partners should preplan to reinforce those measures in grid security emergencies. If the secretary orders utilities to help protect or restore grid reliability beyond their service areas, those orders will help justify (and indeed, legally require) providing such assistance, regardless of the political pressure against doing so. DOE should consider reaching out to state and local leaders and their senior energy appointees before emergencies occur in order to ensure that they are familiar with the FPA requirements and the national security value of mutual assistance.

Emergency orders can also help utilities execute politically unpopular emergency operational decisions within their own service areas. Cyber and physical attacks could put utility CEOs in the unenviable position of having to manage shortfalls in available power by depriving lower-priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The secretary of energy can give CEOs political top cover for taking such unpopular actions, rather than leave them to act on a voluntary basis and bear the full brunt of explaining why they did so.

Exercises can help utilities and government officials prepare to collaborate in the face of intense political pressures, and coordinate the execution of emergency orders on a nationwide basis. NERC already requires BPS entities to exercise their individual emergency and power system restoration plans. In the GridEx exercise series, over one hundred utilities across the

<sup>217</sup> ES&C, "Cyber Mutual Assistance Program."

<sup>218</sup> DOE, *Multiyear Plan*, 29.

<sup>219</sup> EEI, *Understanding the Electric Power Industry's Response and Restoration Process*.



United States and Canada test the use of their plans against combined cyber-physical attacks and exercise the use of Cyber Mutual Assistance protocols and procedures. Building template emergency orders and utility-specific implementation plans will provide an even stronger basis for coordinated multientity exercises. In planning for GridEx V in 2019, NERC and its government and industry partners should consider the possibility of exercising the issuance and implementation of specific template emergency orders. State, local, tribal, and territorial participation in utility exercises that include the use of emergency orders will also be crucial.

### Environmental, Regulatory, and Legal Waivers

In amending the FPA to address grid security emergencies, Congress provided power companies with an important protection for complying with emergency orders—one that they might not receive by implementing equivalent emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate FERC-approved grid reliability standards or other rules or provisions under the FPA, the act specifies that those actions “shall not be considered a violation” of those provisions. Such waivers of enforcement apply unless a complying entity acts in a “grossly negligent manner.”<sup>220</sup>

The FAST Act amendments to the FPA also introduced broader protections into section 202(c), absolving entities from violations of federal, state, or local environmental laws or regulations that occur as a result of complying with an order. That provision shields complying entities from “any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation.”<sup>221</sup> These protections apply to section 215A emergency orders as well.<sup>222</sup>

FPA-based waivers will be especially valuable for certain types of emergency orders. For example, if the secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service, such as proactively shedding firm load, could also violate NERC’s FERC-approved reliability standards.<sup>223</sup> Separating preplanned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards as well.

The waiver process under the FPA is structured to function automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that a BPS entity has acted with gross negligence. Nevertheless, industry, DOE, and regulators might find it useful to build consensus on the types of waivers that specific template orders should include.

Their discussions could also help address more far-reaching regulatory issues that grid security emergencies may pose. For example, the FPA does not provide waivers for Nuclear Regulatory Commission regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the commission would enforce a violation of its regulations by a nuclear generation entity complying with an emergency order. The worst time to adjudicate such a dispute, however, would be in the midst of a grid security emergency. Pre-event discussions will be particularly important given the nuclear fleet’s imperative to protect public health and safety. DOE, the Nuclear Regulatory Commission, and their industry partners will need to ensure that assessments of regulatory issues associated with

<sup>220</sup> 16 U.S.C. § 824o–1, (f)(4).

<sup>221</sup> 16 U.S.C. § 824a, (c)(3).

<sup>222</sup> 16 U.S.C. § 824o–1, (f)(2).

<sup>223</sup> For example, in events such as the September 2011 Arizona–California disturbance, FERC has found that load shedding led to violations of NERC’s reliability standards.

emergency operations take safety considerations into full account.

Preplanning will also be vital for emergency orders that support power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that “the storage of strategically located spare large power transformers” and other critical grid components “will reduce the vulnerability of the United States to multiple risks facing electric grid reliability,” including cyber and physical attacks.<sup>224</sup> Accordingly, Congress required DOE to develop a strategic transformer reserve plan to determine the number and type of spare large power transformers that should be stored and to examine issues associated with transporting those spares.<sup>225</sup>

DOE responded to this requirement by providing a strategic transformer reserve report (March 2017). The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a more substantial pool of spare large power transformers than DOE had anticipated and that a federally owned reserve is not needed.<sup>226</sup> However, the plan also found that it was crucial to ensure that large power transformers can be efficiently moved during national emergencies.<sup>227</sup>

Regulatory waivers can play a critical role in facilitating that movement. The higher-voltage classes of large power transformers, including 765-kilovolt transformers, are as big as a house and can be moved—slowly and very carefully—only by specialized heavy-haul trucks, railcars, and barges. Under the auspices of the ESCC, utilities have established the Transformer Transportation Working Group to analyze the problems posed by moving large power transformers in an emergency

and to build collaborative plans with transportation companies and associations. A central finding of the group’s analysis: regulatory waivers will be critical to expedite the movement of large power transformers, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.<sup>228</sup>

DOE’s 2017 transformer report committed the department to coordinating with the Transformer Transportation Working Group “to improve and optimize transportation planning in response to a significant national event impacting the electricity grid.”<sup>229</sup> However, the report did not examine how emergency orders and implementation plans might speed the transportation of large power transformers. As DOE collaborates with the working group and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols that are not addressed by the FPA and that pose the greatest impediments to transformer movement. DOE and its partners should then preplan to waive these provisions if the secretary issues emergency orders.

The challenge for such preplanning: the secretary of energy lacks the statutory authority to waive key transportation regulations. Most federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of DOT. Federal regulations and emergency operations that would govern the movement of transformers on barges, which could be critical for restoring power for coastal cities and along the Mississippi–Ohio river system of inland waterways, are overseen by the US Coast Guard and the US Army Corps of Engineers. State and local transportation regulations and permitting requirements will also

<sup>224</sup> FAST Act, 1779.

<sup>225</sup> FAST Act, 1780–1782.

<sup>226</sup> DOE, *Strategic Transformer Reserve*, 21.

<sup>227</sup> DOE, *Strategic Transformer Reserve*, 1.

<sup>228</sup> ICF, *Assessment of Large Power Transformer Risk Mitigation Strategies*, 22–23.

<sup>229</sup> DOE, *Strategic Transformer Reserve*, 22.

pose major impediments to moving large power transformers over roads unless adequate waivers are in place to lift restrictions.

DOE should build collaborative plans to employ waiver authorities beyond those directly under the secretary's control. For example, to facilitate the movement of large power transformers, gubernatorial disaster declarations could help waive state-level regulations. The American Association of State Highway and Transportation Officials and National Emergency Management Association are exploring the use of these and other waiver authorities. DOE is also preplanning with other federal, state, local, tribal, and territorial agencies to coordinate response operations under Emergency Support Function #12—Energy.<sup>230</sup> Especially valuable, a growing number of individual power companies are creating contingency plans for emergency transportation with government agencies and road, rail, and barge companies. Building on these efforts, and on initiatives led by the Transformer Transportation Working Group,<sup>231</sup> the electricity subsector and its partners should establish systematic, nationwide plans to facilitate the movement of transformers and other critical equipment in grid security emergencies.

Over the longer term, Congress, industry, and government partners should also consider whether complying entities should have liability protections beyond those currently provided by the FPA. Prioritized load shedding for extended periods will create “winners and losers” in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other section 9+ assets may leave shortfalls in electric service at dialysis centers, small urgent-care centers, and facilities for special-needs citizens. These disruptions will put lives at risk. Legislators, DOE, and electric industry leaders should examine whether utilities complying

with such necessary but highly disruptive emergency orders ought to have additional liability protections. Cutting off power to lower-priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.<sup>232</sup> Again, if these risks of exposure are sufficiently severe, Congress should consider providing further protections for BPS entities.

### **Cost Recovery for Emergency Operations and Support for Investments in Grid Infrastructure**

Complying with emergency orders may force utilities to incur costs beyond their normal operating expenses. The FPA states that if FERC determines “that owners, operators, or users of critical electric infrastructure have incurred substantial costs” in complying with an emergency order, FERC shall “establish a mechanism that permits such owners, operators, or users to recover such costs.”<sup>233</sup> Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other orders could require reimbursement through FERC-directed mechanisms as well.

The act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that emergency orders require utilities responsible for defense critical electric infrastructure to take emergency measures, the “owners or operators” of critical defense facilities that rely on such infrastructure “shall bear the full incremental costs of the measures.”<sup>234</sup> Fair warning to DOD: it

<sup>230</sup> “State and Local Energy Assurance Planning.” DOE.

<sup>231</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>232</sup> Frankel, “Can Customers Sue Power Companies for Outages?”

<sup>233</sup> The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs “prudently” and that those costs “cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users.” 16 U.S.C. § 824o–1, (b)(6)(A).

<sup>234</sup> 16 U.S.C. § 824o–1, (b)(6)(B).

should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- attacks create major blackouts and deprive utilities of revenue;
- emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- adversaries disrupt financial markets, either through direct cyber attacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.<sup>235</sup>

Power companies are strengthening their plans and capabilities for cross-sector support with the financial services sector.<sup>236</sup> These efforts should include the development of contingency plans for financial-services companies (in coordination with the Department of Treasury and DOE) to help utilities cover the urgent expenses they may incur in responding to grid security emergencies. In addition, to facilitate the reimbursement process provided for in the FPA, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with orders will be more difficult once attacks are under way.

Cost recovery for investments in grid infrastructure to facilitate emergency order implementation will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. Other orders may be impossible to execute unless BPS entities make additional investments in infrastructure. It will be near useless to order transmission operators to protect or rapidly restore service to vital but remote military bases served by a single transmission line if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure that these facilities can help defeat US adversaries when the nation is under attack. DOD will need to develop a cost-recovery mechanism to reimburse defense critical electric infrastructure owners for making such investments.

To be even remotely viable as an emergency order design option, most preplanned power islands will also require at least some infrastructure construction. Ideally, these preplanned islands will use existing generation, transmission, and distribution assets within their service footprints to separate from the grid and still be able to provide reliable electric service to the section 9+ assets inside their borders. But many areas that might be designed to function as islands in a grid security emergency will lack adequate infrastructure to do so. The grid's interconnected design enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Preplanned power islands will not only lose those reliability benefits, but they will also have to make do with infrastructure that utilities built and aligned to be supporting components of the interconnected grid—not self-sustaining islands that would be stood up in grid security emergencies. Moreover, operating and recovering from preplanned island schemes will create an entirely different operating mode than industry is currently designed

<sup>235</sup> NERC, *GridEx III Report*, 15.

<sup>236</sup> See, for example, the Strategic Infrastructure Coordinating Council (SICC). ESCC, "ESCC: Electricity Subsector Coordinating Council."



for. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: to be effectively implemented, many emergency orders could require spending on new transmission lines and other grid infrastructure.

The FPA provisions for grid security emergencies do not explicitly authorize reimbursement for infrastructure investments. While the act requires FERC to establish a mechanism to enable owners, users, and operators of critical and defense critical electric infrastructure to recover their costs of complying with emergency orders, those funding provisions do not mention preattack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover costs for infrastructure investments in resilience against cyber and physical attacks.<sup>237</sup> FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate emergency order execution.

Similar discussions will be necessary with state public utility commissions. As noted above, local distribution systems will play vital roles in implementing emergency orders. Public utility commissions have primary regulatory authority over such distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. They could also make important contributions to reviewing proposed implementation plans for emergency orders that would be executed within their respective states, particularly when local distribution systems would be necessary to implement the orders.

<sup>237</sup> See, for example, FERC, *Extraordinary Expenditures* (96 FERC ¶ 61,299), 1; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), 10–11; and FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), 60.

The FPA opens the door to such discussions. The act states that FERC and the secretary of energy “shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions.”<sup>238</sup> Initiating these discussions with the National Association of Regulatory Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has extensively analyzed criteria for assessing the prudence of investments against cyber and physical attacks and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

## Conclusions and Recommendations for Broader Progress

Taken together, the options for industry–government collaboration examined in this report constitute a massive undertaking for which Congress appropriated zero funding to utilities. Developing a sequenced, prioritized strategy to explore these options will help make doing so a more manageable task.

Potential emergency orders will differ not only in terms of the phases of an attack in which they would be most useful, and in the degree to which they will disrupt normal electric service, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create—especially those that fall into the no-regrets category. Utilities frequently use conservative operations to help protect grid reliability in severe weather events. A growing number of companies are

<sup>238</sup> 16 U.S.C. § 824o–1, (d)(4).



already building on that foundation to draft equivalent conservative operations against cyber and physical threats. Emergency orders based on these initiatives constitute “low-hanging fruit”; creating such orders offers an immediate opportunity for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging emergency order initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are under way, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. Improving communications survivability and preplanning to counter disinformation campaigns will also be crucial for grid security emergency preparedness. So, too, will be efforts not only to fully leverage the FPA’s regulatory waiver and cost recovery mechanisms but also to explore additional liability protections and other measures to help entities comply with emergency orders.

A comprehensive plan to align and integrate these initiatives should also address three additional opportunities to build resilience for grid security emergencies: (1) preplanning to use additional federal and state emergency authorities to defend natural gas systems, communications networks, and other infrastructure on which the grid depends; (2) coordinating with Canada, Mexico, and other nations whose grids may be struck in conjunction with attacks on US electric systems; and (3) exploring new options to deter and defeat attacks on the grid by integrating defensive measures with government operations to blunt further strikes on US power companies and other targets.

## Employing Additional Emergency Authorities for Cross-Sector Resilience

Building preparedness against attacks on the grid is necessary but not sufficient to protect BPS reliability. In many US regions, power generation is becoming extraordinarily dependent on the flow of natural gas. Adversaries may attempt to cause cascading blackouts and other major grid instabilities by crippling natural gas systems. To hedge against such disruptions, some generators have the ability to operate on diesel and other secondary fuels if attackers interrupt gas supplies. But the refining and transportation systems needed to resupply such “dual-fuel” generators with diesel will themselves be at risk in grid security emergencies.<sup>239</sup> Moreover, as examined earlier in this report, coordinated grid restoration will also depend on the availability of communications systems and other infrastructure sectors.

This report has focused on employing the emergency authorities that Congress incorporated into the FPA by creating section 215A of the act in 2015. However, these authorities apply only to BPS owners and operators. The secretary cannot issue emergency orders under 215A to operators of natural gas and diesel fuel systems, much less to telecommunications companies and other infrastructure owners beyond the energy sector. The secretary has a range of other emergency authorities, including the Defense Production Act (DPA) and the authorities provided by section 202(c) of the FPA, which could facilitate coordinated response and restoration operations across the energy sector. The analysis that follows examines how DOE and its industry partners could preplan for the integrated use of all such authorities in a grid security emergency. This analysis also examines how federal and state leaders might use additional emergency powers to coordinate multisector response operations.

<sup>239</sup> The author has advised Exelon Corporation on risks of fuel interruptions for power generation. Exelon has provided no funding for this report.

## Coordinating Emergency Operations among Electric Utilities, Natural Gas Systems, and Other Energy Sector Components

Natural gas is an increasingly important source of fuel for power generation in many regions of the United States. Between 2002 and 2016, the nationwide share of electricity provided by gas-fired units increased from 18 percent to approximately 34 percent.<sup>240</sup> However, in New England, California, and other parts of the United States, natural gas has become the predominant source of fuel for power generation.

ISO New England has highlighted the risks that this reliance creates for grid resilience. It notes that “in New England, the most significant resilience challenge is fuel security—or the assurance that power plants will have or be able to obtain the fuel they need to run, particularly in winter—especially against the backdrop of coal, oil, and nuclear unit retirements, constrained fuel infrastructure, and the difficulty in permitting and operating dual-fuel generating capability.”<sup>241</sup>

Other regions also face growing fuel supply risks to grid resilience. A DOE-sponsored report titled *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units, Volume I: The Critical Role of Thermal Units During Extreme Weather Events* (March 2018) notes that many regional transmission organizations and independent system operators will face a combined challenge of inadequate natural gas pipeline infrastructure and competing demands for fuel from users apart from power generators.<sup>242</sup> More broadly, NERC has found that “the electric sector’s growing reliance on natural gas raises concerns regarding the ability to maintain BPS reliability when facing constraints on the natural

gas delivery systems.”<sup>243</sup> NERC’s 2016 *Long-Term Reliability Assessment* also notes that “as part of future transmission and resource planning studies, planning entities will need to more fully understand how impacts to the natural gas transportation system can impact electric reliability.”<sup>244</sup> Additionally, in *Grid Resilience in RTOs and ISOs* (January 2018), FERC called for additional data to better assess the risks posed by “wide-scale disruption to fuel supply” that could result in outages of multiple generators.<sup>245</sup>

Companies in the oil and natural gas subsector are bolstering their capabilities to protect their critical system components from attack and are taking new measures to ensure the continued safe and reliable delivery of natural gas to critical customers, including power generators.<sup>246</sup> However, threats to the oil and natural gas subsector are rapidly escalating as well.<sup>247</sup> As gas system owners and operators address these increasing threats, new opportunities will emerge for joint gas–electric resilience initiatives and emergency planning.

The oil and natural gas and electricity subsectors are already improving their coordination on resilience issues.<sup>248</sup> Moreover, NERC has been facilitating coordination between BPS entities and natural gas companies to address fuel resilience and interdependency challenges.<sup>249</sup> The ESCC has also been developing new coordination mechanisms for the

<sup>240</sup> DOE, *Staff Report to Secretary*, 90.

<sup>241</sup> ISO-NE, “Response of ISO New England Inc.,” 1.

<sup>242</sup> NETL, *Reliability, Resilience and the Oncoming Wave*, 4, 14, 22, 3.

<sup>243</sup> NERC, *Short-Term Special Assessment*, 12. See also NERC, *2013 Special Reliability Assessment*.

<sup>244</sup> NERC, *2016 Long-Term Reliability Assessment*, 21.

<sup>245</sup> FERC, *Grid Resilience*, 161 FERC ¶ 61,012 (2018), 14. See also Stockton, *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*.

<sup>246</sup> “Cybersecurity,” American Gas Association.

<sup>247</sup> Sobczak, Northey, and Behr, “Cyber Raises Threat”; and Stockton (on behalf of Exelon Corporation), *Prepared Direct Testimony* (Docket No. RM18-1-000), 13.

<sup>248</sup> DOE, *Staff Report to Secretary*, 94; and EIS Council, *E-PRO Handbook II*, 189.

<sup>249</sup> NERC, *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*, 1.

two industries (as well as with communications and financial services sectors).<sup>250</sup> Additionally, the natural gas industry participated in GridEx IV, which examined opportunities to mitigate the risk that adversaries will simultaneously attack gas and electric systems.

Building on these and other collaborative efforts, gas and electric companies (and their regulatory partners) should examine how they can prioritize support for each other in grid security emergencies. For example, when blackouts occur, electric companies typically prioritize the restoration of service to compression stations and other electricity-dependent gas infrastructure that is essential to supply fuel for power generation and other critical customers. Support for gas infrastructure should remain a priority, even as BPS entities add other section 9+ facilities to their restoration plans. Gas companies might also reassess their curtailment policies to help gas-dependent BPS entities sustain service to major military installations and other vital facilities in grid security emergencies.<sup>251</sup>

BPS entities and DOE should also pursue deeper collaboration with the companies that refine and deliver secondary fuels for power generation. If adversaries interrupt the flow of natural gas, dual-fuel generators can use diesel, no. 2 fuel oil, or other secondary fuels to sustain their operations in a grid security emergency.<sup>252</sup> However, cascading blackouts could disrupt the flow of these secondary fuels as well. Refining and transportation systems components that are essential to resupply dual-fuel generators depend on electricity. Adversaries may also attack these systems at the same time they strike the grid. Moreover, ongoing cutbacks in industry delivery capacity could magnify these risks of interruption. ISO New England notes that a “withering

delivery supply chain” constitutes an “unquantifiable X factor” in assessing grid resilience.<sup>253</sup> Preplanning to prioritize the delivery of secondary fuels for power generation will be essential for grid security emergencies, especially given the enormous demand for diesel from emergency power generators from hospitals, water utilities, and other vital facilities in wide-area blackouts.

Emergency authorities beyond 215A can help prioritize the flow of natural gas and secondary fuels to protect and restore grid reliability. The DPA will be especially helpful in this regard. The act is the “primary source of presidential authority to expedite and expand the supply of critical resources from the U.S. industrial base to support the national defense and homeland security.”<sup>254</sup> The DPA defines national defense to include “critical infrastructure protection and restoration,” encompassing all electric system components and supporting fuel supply infrastructure (including natural gas pipelines) that are at risk of cyber and physical attacks.<sup>255</sup> In 2012, the White House delegated many of the president’s DPA authorities to the heads of relevant federal agencies, including the secretary of energy for prioritization and allocation decisions regarding “all forms of energy.”<sup>256</sup>

Especially valuable for cross-sector resilience, DOE has established an Energy Priorities and Allocations System that enables the department to prioritize contracts for the delivery of natural gas, diesel, and other energy resources between the companies that provide them and government agencies, electric utilities, and other private and public sector customers. The system also enables DOE to allocate energy materials, services, and facilities to promote

<sup>250</sup> ESCC, “ESCC: Electricity Subsector Coordinating Council.”

<sup>251</sup> EIS Council, *E-PRO Handbook II*, 219.

<sup>252</sup> ISO-NE, *Operational Fuel-Security Analysis*, 52; and NERC, *2013 Special Reliability Assessment*, 4.

<sup>253</sup> ISO-NE, *Operational Fuel-Security Analysis*, 14, 16.

<sup>254</sup> DHS, *Power Outage Incident Annex*, 129.

<sup>255</sup> 50 U.S.C. § 4552, (14).

<sup>256</sup> Obama, *Executive Order—National Defense Resources Preparedness*.

“critical infrastructure protection and restoration” and emergency preparedness.<sup>257</sup>

DOE has already used its authorities under the DPA to support power generation in previous energy crises. In 2001, for example, the department used these authorities to ensure that emergency supplies of natural gas continued to flow to Californian power generators, thereby helping to avoid threatened electrical blackouts.<sup>258</sup> Now, to build preparedness for grid security emergencies, DOE and its industry partners should consider preplanning to use the DPA to sustain or restore gas and diesel deliveries to critical generators, including those that serve microgrids on defense installations, regional hospitals, and other assets critical for national security and public health and safety.

DOE could use the DPA to support and prioritize power restoration operations in other ways as well. Section 101(a) of the act provides DOE with the authority to prioritize the delivery of critical grid components in an emergency. If coordinated physical attacks damage or destroy transformers at a large number of critical substations, the secretary could use the DPA to allocate replacement transformers in ways that most directly benefit national security and public health and safety.

Two additional sources of emergency authorities could further strengthen preparedness and supplement the use of section 215A emergency orders. The first is section 202(c) of the FPA. The section authorizes the secretary to order “temporary connections of facilities and such generation, delivery, interchange, or transmission of electric energy as in its judgment will best meet the emergency and serve the public interest.” That provision also specifies that the secretary could exercise such powers “during the continuance of any war in which the United States is engaged, or whenever the Commission determines that an

emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy or of facilities for the generation or transmission of electric energy, or of fuel or water for generating facilities, or other causes.”<sup>259</sup>

A key virtue of section 202(c) is that the secretary can apply these emergency authorities to local distribution systems that might not fall within the purview of section 215A. Moreover, DOE has a strong record of having used 202(c) authorities in past emergencies, including the California Enron crisis, Hurricane Katrina, and other events.<sup>260</sup> DOE and its industry partners should consider building on this foundation to plan for the use of these authorities in grid security emergencies.

The Natural Gas Policy Act provides further authorities that could help coordinate energy sector operations in grid security emergencies. The president must declare a natural gas supply emergency before the secretary gains emergency powers under the act. The president can make such a declaration if there is evidence of an imminent or existing “severe natural gas shortage, endangering the supply of natural gas for high-priority uses” and that, having exhausted other alternatives “to the maximum extent practicable,” natural gas emergency authorities are necessary to resolve the situation.<sup>261</sup> The president may also delegate this authority, as well as the authority to issue rules or orders, to the secretary of energy or other appropriate federal officials.<sup>262</sup>

The president or secretary can issue two main types of orders or rules. Most important, during a natural gas supply emergency, the act authorizes the president or other officials to allocate natural gas supplies “to assist in meeting natural gas requirements for high-priority

<sup>257</sup> DOE, “RIN 1901-AB28,” 33615, 33622-33626.

<sup>258</sup> Brown and Else, *Defense Production Act of 1950*, 10.

<sup>259</sup> 16 U.S.C. § 824a, (c)(1).

<sup>260</sup> “DOE’s Use of Federal Power Act Emergency Authority,” DOE.

<sup>261</sup> 15 U.S.C. § 3361, (a).

<sup>262</sup> 15 U.S.C. § 3364, (d).



uses.”<sup>263</sup> The secretary could use this provision to ensure that critical generating facilities get the fuel they need.

Of course, some of these authorities overlap. DOE and its government and industry partners should develop an integrated approach to employing these powers for grid security emergencies, and determine which particular authorities are best suited to meet specific energy sector risks that cyber and physical attacks can create. These partners, along with other energy sector stakeholders, should also consider exercise scenarios that involve the simultaneous use of multiple emergency authorities to simulate the complex legal environment they may be faced with in a grid security emergency.

### **Multisector Resilience for Grid Security Emergencies**

An overarching strategy for grid security emergency preparedness should also advance operational coordination between energy companies and other infrastructure sectors that both rely on electricity and play vital roles in power restoration. Additional federal emergency authorities and incident response plans can help strengthen coordination between these interdependent sectors.

Using this broader array of plans and authorities will be particularly important if adversaries simultaneously attack multiple infrastructure sectors. By striking other sectors together with the grid, adversaries can exploit interdependencies between them to maximize the attack’s disruptive effects on national security, including the ability of defense installations and supporting civilian infrastructure to conduct operations abroad.<sup>264</sup> The *National Cyber Incident Response Plan* provides a framework for strengthening multisector coordination mechanisms for such attacks. As the administration refines the

plan, DOE and its government and industry partners should ensure that the issuance and execution of emergency orders fit within this broader framework and directly contribute to multisector resilience.

Updates to the *National Response Framework* and other FEMA-led initiatives can offer further benefits for grid security emergencies. In its after-action report from the 2017 hurricane season, FEMA noted that emergency managers and their private sector partners lack the multisector coordination mechanisms necessary to accelerate the restoration of electric power and other lifeline services.<sup>265</sup> The report called for FEMA to build “a cross-sector approach to the Agency’s planning, organizing, response, and recovery operations,” and revise current national-level planning frameworks to create a cross-sector emergency support function.<sup>266</sup> DOE and industry should partner to prioritize support for power sustainment and restoration within this broader initiative.

The *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans* provides a prime opportunity to embed cross-sector coordination efforts in regional incident response plans.<sup>267</sup> The annex calls for the development of regional plans to build resilience against extended multistate blackouts and ensure that interdependent sectors can accelerate power restoration while also countering threats to public health and safety.<sup>268</sup> In many areas of the United States, utilities are already helping DOE, FEMA, and their state and local partners build such plans for their regions. Cross-sector preparedness for grid security emergencies should become a key focus of future power outage incident planning efforts.

<sup>263</sup> 15 U.S.C. § 3363, (a).

<sup>264</sup> Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee*, 11.

<sup>265</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 13.

<sup>266</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 12–13.

<sup>267</sup> EIS Council, *E-PRO Handbook III*, 45.

<sup>268</sup> DHS, *Power Outage Incident Annex*, 77.



In all of these planning and operational coordination initiatives, DOE and other departments responsible for specific infrastructure sectors should examine how other federal emergency authorities might supplement those that apply to the energy sector. The communications sector provides one such opportunity. The president has extensive authorities to address national security and emergency preparedness telecommunications issues under the Communications Act, including the power to prioritize the use of communications capabilities and provide complying entities with legal and regulatory protections.<sup>269</sup> Executive Order 13618 assigns many of these authorities and associated responsibilities to federal departments and agencies. The secretary of commerce, for example, is responsible for developing plans and procedures for emergency use of radio frequencies and other communications systems.<sup>270</sup> The secretary of homeland security is responsible for overseeing the development, testing, and implementation of emergency communications capabilities.<sup>271</sup> Using these capabilities to support power restoration could be enormously helpful in grid security emergencies. Equivalent emergency authorities for other sectors could assist restoration as well. However, as with all such opportunities, effectively using these federal authorities will depend on extensive preplanning.

State governors are likely to invoke their own authorities to respond to grid security emergencies. Governors have primary responsibility for protecting the health and safety of their citizens. Cyber and physical attacks on the grid, especially if paired with strikes against communications systems and other interdependent sectors, could disrupt hospitals, water systems, and other assets on which their citizens rely. Governors in every state have the ability to declare emergencies and issue executive orders to help deal

with such threats to public health.<sup>272</sup> A growing number of states are also including utility representatives in their emergency operations centers, building collaborative plans and coordination mechanisms to respond to attacks on the grid, and preparing for state National Guard personnel to help utilities defend and restore the flow of power. These initiatives are bolstering overall preparedness for grid security emergencies. However, if multiple governors employ their own emergency authorities and implement state-level blackout response plans, it will be enormously difficult to coordinate their efforts with federal actions—including the issuance of DOE emergency orders to utilities in those very same states.

The only way to overcome such difficulties is to exercise the use of all of the authorities that could help protect and restore grid reliability, across multiple sectors and with the participation of both federal and state leaders. GridEx IV offered an important step forward in this regard. Exercise participants from the oil and natural gas subsector, as well as the financial-services and communications sectors, contributed perspectives on how they could help utilities respond to cyber and physical attacks on the grid. Representatives from state governments discussed how governors might act in such an emergency. GridEx V will provide an opportunity to address such coordination challenges in greater detail. GridEx V could also exercise the use of specific template emergency orders, together with communications mechanisms and playbooks developed for grid security emergencies. Additional exercises by BPS entities and their partners at all levels of government will also be vital to prepare for the implementation of such orders.

## Extended Partnership Requirements within the United States and Abroad

Congress implicitly imposed geographic constraints on the secretary's authority to issue emergency orders to protect the reliability of defense critical electric

<sup>269</sup> 47 U.S.C. § 606.

<sup>270</sup> Obama, *Executive Order—Assignment*, section 5.3.

<sup>271</sup> Obama, *Executive Order—Assignment*, section 5.2. See also DHS, “Emergency Communications.”

<sup>272</sup> Orenstein and White, “Emergency Declaration Authorities.”

infrastructure. The FPA limits such infrastructure to that which is located in the forty-eight contiguous states or the District of Columbia.<sup>273</sup> However, Alaska and Hawaii are home to vital grid-dependent military installations and supporting civilian infrastructure, including facilities for US continental ballistic missile defense and command and control of military operations in the Pacific region. Key defense installations also exist in Guam and other US territories. As the electric industry and DOE build preparedness for grid security emergencies, they should consider collaborating with the utilities that serve these states and territories and their government partners (including DOD) to strengthen plans and capabilities for coordinated operations.

Close coordination will also be necessary with Canada. The secretary of energy has no authority to issue emergency orders to power companies in other countries. However, the electric grids of the United States and Canada are deeply interconnected. This integration entails both risks and opportunities in grid security emergencies. Adversary-induced blackouts in one nation may cascade across the border, and extraordinary measures taken to restore US grid reliability could affect Canadian systems. Yet, the connectivity between US and Canadian electric systems can also provide unique opportunities to strengthen the security and emergency preparedness of both nations.

A key foundation for binational cooperation in grid security emergencies is already in place. NERC's reliability standards apply to both US and Canadian utilities, providing shared planning and emergency coordination mechanisms on both sides of the border. US and Canadian power companies and government officials should explore how they might supplement these existing mechanisms for

grid security emergencies. The most immediate opportunity to do so will lie in government-to-government consultations. The FPA requires that, to the extent practicable, the secretary of energy shall consult with Canadian authorities before issuing emergency orders.<sup>274</sup> However, the FPA provides no details on the mechanisms by which consultations will be conducted or on whether and how Canadian officials should be informed when the secretary issues emergency orders to US utilities. The analysis that follows examines opportunities to facilitate binational consultation and operational coordination in grid security emergencies.

The FPA also requires that the secretary consult with the Mexican government before issuing emergency orders. While the US and Mexican grids are much less integrated than those of the US and Canada, discussions on grid security emergency preparedness with Mexican officials could also be valuable. Coordination beyond North America may be useful as well. If a severe regional crisis escalates into attacks on the US power grid, US security partners in those regions may face strikes against their own electric systems. Sharing information on whether an attack is imminent and taking coordinated grid protection measures (including those for conservative operations) will help the United States and its allies meet such challenges.

### **Deepening Integration between US and Canadian Grids: Risks and Potential Benefits for Grid Security Emergency Resilience**

DOE notes that "the United States and Canada serve as a global model of highly functional, cross-border electricity coordination."<sup>275</sup> US and Canadian grids are connected by over three dozen major transmission lines, ranging from the Pacific Northwest to New England. The resulting power flows have created a deeply integrated network of north-south BPS infrastructure and synchronized

<sup>273</sup> 16 U.S.C. § 824o-1, (a)(4). The FPA's section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).

<sup>274</sup> 16 U.S.C. § 824o-1, (b)(3).

<sup>275</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-5.

cross-border operations.<sup>276</sup> This integration also provides significant economic and energy security benefits for both countries.<sup>277</sup>

Connectivity between US and Canadian grids will grow still closer in the decades to come.<sup>278</sup> New York and Massachusetts are pursuing significant increases in Canadian hydropower to help achieve their clean energy goals. Several new cross-border transmission lines are also under development, though many of them face permitting challenges. The Lake Erie Connector is a one-thousand-megawatt high-voltage, direct current line expected to link Ontario's Independent Electricity System Operator with PJM in 2020.<sup>279</sup> The Champlain Hudson Power Express from Quebec to New York City is expected to go into service in 2021, with still other projects in various phases of development in New England, the Midwest, and the Pacific Northwest.<sup>280</sup>

These and other projects offer significant economic benefits to both nations. However, the connectivity of US and Canadian power grids also creates risks of cross-border failures. The 2003 Northeast blackout that started in Ohio created power outages for millions of customers in Ontario.<sup>281</sup> Interconnections between US and Canadian power systems have increased since that event. US and Canadian officials warn that given this connectivity, "isolated or complex events with cascading effects that take place in either country can have major consequences for both the United States' and Canada's electric grids and adversely affect national security, economic stability, and public health and safety."<sup>282</sup>

Mandatory reliability standards reduce the risks of outages across North America. In the aftermath of the 2003 blackout, NERC began issuing standards applicable to entities on both sides of the border. NERC reliability standards are mandatory and enforceable in the provinces of Ontario, New Brunswick, Alberta, British Columbia, Manitoba, and Nova Scotia. Twelve such reliability standards also went into effect in Quebec in April 2015; the province is now considering adopting additional standards.<sup>283</sup> These shared US-Canada standards help power companies in both countries maintain the reliability of their systems and will help them prevent instabilities from spreading during grid security emergencies.

NERC's role as the electric reliability organization for North America provides an additional bulwark for binational grid resilience. As Figure 7 illustrates, three NERC regional entities include power companies on both sides of the border: the Northeast Power Coordinating Council (NPCC), the Midwest Reliability Organization (MRO), and the Western Electricity Coordinating Council (WECC). These entities help monitor and enforce compliance with reliability standards and reinforce NERC's integrated approach to reducing the risks of cascading failures and other instabilities.<sup>284</sup> The E-ISAC also provides additional support for utility preparedness in both nations.

However, Russia and other potential adversaries' increasingly sophisticated cyber capabilities pose challenges for protecting power flows between Canada and the United States, just as they do for electric service within each country individually.

Connectivity between US and Canadian power systems offers other benefits for protecting reliability against cyber and physical attacks. For example, as

<sup>276</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-6.

<sup>277</sup> Stanley, *Mapping the U.S.-Canada Energy Relationship*, 9.

<sup>278</sup> Parfomak et al., *Cross-Border Energy Trade*, 34.

<sup>279</sup> "Work Continues on ITC Lake Erie Project," *Transmission Hub*.

<sup>280</sup> Vine, *Interconnected: Canadian and U.S. Electricity*, 9.

<sup>281</sup> NERC Steering Group, *Technical Analysis of Blackout*, 1.

<sup>282</sup> Governments of US and Canada, *Joint United States-Canada Electric Grid Security and Resilience Strategy*, 10.

<sup>283</sup> "North America," NERC. See also "Compliance - Québec," Northeast Power Coordinating Council; and "Electric Power Transmission Reliability Standards," Régie de l'énergie Québec.

<sup>284</sup> "Key Players," NERC.

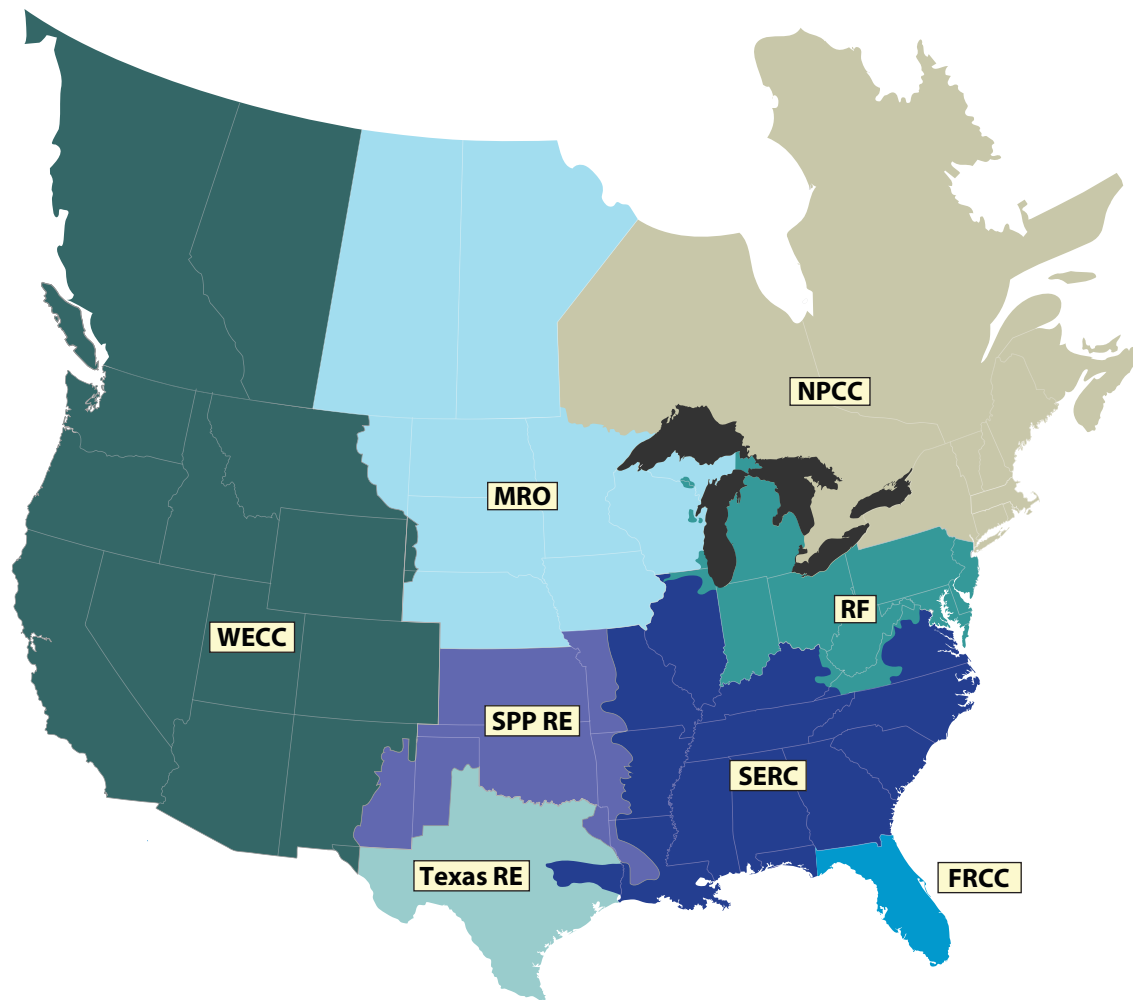


Figure 7. NERC Regional Entities across North America

new transmission lines increase this connectivity, electricity exported by Canada could become increasingly valuable when managing power imbalances in the United States and could make up for sudden shortfalls in the availability of US-generated power. However, we must assume that adversaries know this as well. To maximize the disruption to the US grid and the critical facilities that depend on it, attackers may strike the cross-border transmission lines that would otherwise help US grid owners and operators prevent cascading failures, uncontrolled separations, and other major reliability issues.

Adversaries may also attack grid assets that supply power to critical Canadian defense installations. The United States and Canada have a unique binational

defense system to protect their territories. The North American Aerospace Defense Command plays a vital role for both nations for aerospace warning, aerospace control, and maritime warning for North America.<sup>285</sup> The Canada-US Civil Assistance Plan also helps enable military members from one nation assist the other's armed forces in support of civilian authorities during emergencies.<sup>286</sup> Potential adversaries such as Russia may seek to degrade these binational military capabilities and operations by attacking defense critical electric infrastructure on

<sup>285</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

<sup>286</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.



both sides of the border. US and Canadian officials and power companies should plan accordingly for mutual support in grid security emergencies.

### Specific Options for US–Canada Coordination

In addition to requiring US–Canada consultations before the secretary issues emergency orders, the FPA also states that FERC and the secretary “shall, in consultation with Canadian and Mexican authorities, develop protocols for the voluntary sharing of critical electric infrastructure information with Canadian and Mexican authorities and owners, operators and users of the bulk-power system outside the United States.”<sup>287</sup> Those initiatives provide a valuable starting point to build shared North American preparedness for grid security emergencies. However, much deeper collaboration is both possible and necessary, especially with Canada. Options for further analysis are described below.

**Consultative mechanisms, collaborative planning, and coordinated emergency operations.** The FPA does not specify how US officials would consult with their Canadian counterparts if the president declares a grid security emergency. Nor does it discuss whether the president would do so prior to making such a declaration. Exchanges between the US president and the prime minister of Canada would constitute the highest level of binational coordination. More detailed discussions about options for responding to incidents could also occur between the secretary of energy and the Canadian minister of national resources. That minister has the federal lead for electricity issues in Canada but lacks emergency authorities equivalent to those that the FPA grants to the secretary of energy.<sup>288</sup>

However, government coordination mechanisms will also need to include a broader array of participants. Global Affairs Canada and the US State Department might well be involved in any coordination of

binational grid emergency actions, just as they are in other emergency assistance mechanisms.<sup>289</sup> Coordination with state and provincial governments could also be helpful. The 1982 amendments to Canada’s Constitution Act (1867) explicitly recognized provinces’ and territories’ constitutional rights to manage electrical energy.<sup>290</sup> In particular, authority over electricity generation and transmission in Canada rests primarily with provincial governments.<sup>291</sup> It will be essential to account for these features of Canadian governance in building US–Canada consultative mechanisms.

The NERC alert system and other emergency coordination systems provide a solid basis for collaboration between US and Canadian utilities in grid security emergencies. However, the FPA does not address the question of how (and how much) information DOE officials should share with Canada on the issuance of emergency orders to US utilities. Given the deep integration of the US and Canadian grids, maximum sharing could help coordinate both countries’ emergency operations before, during, and after attacks. To facilitate such information sharing, DOE, Natural Resources Canada, and other relevant stakeholders can leverage existing US–Canadian mechanisms to protect sensitive information, supplemented as needed to support grid security emergency coordination.

The *Joint US-Canada Electric Grid Security and Resilience Strategy* (December 2016) provides a policy framework for building these coordination and information sharing mechanisms. The US and Canadian governments developed the strategy “to strengthen the security and resilience of the U.S. and Canadian electric grid from all adversarial, technological, and natural hazards and threats.”<sup>292</sup> The strategy calls for collaboration to protect system assets and

<sup>287</sup> 16 U.S.C. § 824o–1, (d)(5).

<sup>288</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>289</sup> “Compendium,” Public Safety Canada.

<sup>290</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>291</sup> “North America,” NERC.

<sup>292</sup> Governments of US and Canada, *US-Canada Electric Grid Security and Resilience Strategy*, 1.



critical functions in both nations so that the North American grid can “withstand and recover rapidly from disruptions.”<sup>293</sup> The strategy also emphasizes the need for collaboration to manage contingencies and enhance response and recovery efforts.<sup>294</sup> All of these features make the strategy a promising basis for creating the detailed collaborative mechanisms that grid security emergencies will require.

### **Protecting defense critical electric infrastructure.**

While the FPA facilitates the development of emergency orders to protect the flow of power to critical US defense installations, US–Canada coordination in grid security emergencies could also help strengthen power resilience for bases on both sides of the border. The Pacific Northwest exemplifies the potential benefits of such collaboration. Washington State hosts a number of vital installations, including Joint Base Kitsap on Puget Sound, which serves as the homeport for aircraft carriers, attack submarines, and other assets that would be needed for operations in the South China Sea and for other regional contingencies. Canadian Forces Base Esquimalt and other key Canadian installations are located less than one hundred miles away on Vancouver Island. Esquimalt is the second-largest military base in Canada and is home to Maritime Forces Pacific and Joint Task Force Pacific headquarters.<sup>295</sup> Coordinating US–Canada emergency plans to protect the flow of power to these installations could benefit the security of both nations.

The US–Canada Permanent Joint Board on Defense provides an ideal venue to explore such coordination options. Established in 1940 to discuss and advise on issues related to continental defense and security, the board has focused increasing attention on binational opportunities to strengthen critical infrastructure resilience. In 2011, the CEO of NERC led a

Permanent Joint Board on Defense discussion of how North American BPS emergency plans and coordination mechanisms could benefit US and Canadian national security. Natural Resources Canada and DOE have also participated in subsequent Permanent Joint Board on Defense meetings, along with the defense departments of both nations and critical infrastructure stakeholders. US and Canadian officials should consider using the board to facilitate industry–government discussions on opportunities to coordinate in grid security emergencies.

### **Coordination with Mexico and Beyond: Multinational Resilience against Grid Security Emergencies**

The US grid has much less connectivity with Mexican electric systems than with the Canadian grid. Southern California and a portion of Mexico’s Baja California have synchronous interconnections. Along the Mexico–Texas border, asynchronous interconnections also exist between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities.<sup>296</sup> In 2017, Mexican and US officials agreed to nonbinding pledges to increase this connectivity in ways that would strengthen reliability on both sides of the border.<sup>297</sup>

The election of Mexican president Andrés Manuel López Obrador in July 2018 may lead to significant changes in that country’s energy policies.<sup>298</sup> Structural challenges will also slow efforts to increase US–Mexico grid integration, including repeated power shortages and major shortfalls in the functionality of the Mexican grid.<sup>299</sup> Nevertheless, it could be useful to expand discussions with industry and the incoming government on protecting grid reliability against cyber and physical threats.

<sup>293</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 12.

<sup>294</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 11.

<sup>295</sup> “Maritime Forces Pacific,” Royal Canadian Navy.

<sup>296</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–4.

<sup>297</sup> “Increasing Electricity Cooperation in North America,” DOE.

<sup>298</sup> Kissane and Medina, “Energy Aftershocks.”

<sup>299</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–13.

Building grid security emergency coordination mechanisms beyond North America would also be helpful. As noted earlier, attacks on the US grid are most likely to occur in the context of an intense, escalating regional crisis in the Baltics, Northeast Asia, or some other area where US allies and critical security interests are at risk. In particular, adversaries may seek to inflict blackouts that could disrupt the deployment of US forces to the crisis zone. But we should also expect that US allies in the region will suffer attacks on their own grids, aimed at disrupting their ability to conduct combined operations with the United States and deliver electricity to US bases on their territories.

NATO's 2018 Locked Shields exercise focused on building alliance-wide preparedness for cyber and physical attacks against energy and communications systems.<sup>300</sup> In future exercises, allies might explore how to jointly determine whether grid attacks are potentially imminent and coordinate on the implementation of conservative operations across NATO member countries. The United States might explore equivalent opportunities for collaboration with Japan, South Korea, Australia, New Zealand, and other security partners. Existing treaty commitments, including those under Article V of NATO's founding treaty, will provide a starting point to meet our shared grid resilience challenges.<sup>301</sup>

### Playing Defense in Cyberwarfare: Doctrine, Integrated Planning, and Benefits for Deterrence

Utility leaders are urging the federal government to do more to assist them in deterring and defeating attacks on the grid. Their calls come at a perfect time. Administration officials have opened the door to new forms of operational collaboration between industry and government, including "collective

defense" during cyber attacks.<sup>302</sup> This report examines an especially significant option to expand their collaboration: coordinating the implementation of emergency orders with DOD operations to halt attacks at their source.

Deeper operational partnerships can also help meet underlying challenges for cyber deterrence. A number of cybersecurity analysts argue that deterrence by denial is impractical in cyberspace because offensive cyber capabilities are so much stronger than cyber defenses, and because cyber warfare will be very different from conventional conflicts. Analysts also warn that the United States lives in a cyber "glass house": given the vulnerability of the power grid and other infrastructure systems, the president cannot credibly threaten to use cyber weapons to defend US allies and interests. Improving preparedness for grid security emergencies can help address these concerns and support ongoing reassessments of US strategies for deterrence.

### Unity of Effort in Defensive Operations at Home and Abroad

Tom Fanning, CEO of Southern Company (one of the largest power companies in the United States), notes that he and other infrastructure owners and operators face a major constraint on their ability to defend their systems: "I can't fight back."<sup>303</sup> In theory, blunting attacks at their source could greatly ease the scale and severity of the threats that utilities will need to counter. In practice, integrating grid security emergency operations with measures to suppress enemy attacks would entail major policy and technical obstacles.

Power companies should not be responsible for striking enemies' offensive cyber infrastructure during grid security emergencies. The US government is the sole actor with the prerogative to engage in techniques such as "hacking back" that

<sup>300</sup> Cowan, "Locked Shields 2018."

<sup>301</sup> "The North Atlantic Treaty," NATO.

<sup>302</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>303</sup> Smith, "U.S. Officials Push New Penalties."

involve operations to disrupt or destroy an attacker's system.<sup>304</sup> Moreover, even if power companies gained legal authority to fight back against adversaries, their technical capacity to do so would be dwarfed by the capabilities possessed by US Cyber Command and other US government organizations.

Efforts to integrate defensive operations at home and abroad should rest on the comparative advantages of industry and government. BPS entities and other components of the electricity subsector are best positioned to defend their systems from within, assisted by DOE and other government partners. Operations abroad to halt attacks on the grid should remain the exclusive purview of government agencies, supported by industry assistance to gather malware samples and facilitate attack attribution. Based on this division of labor, government and industry leaders could explore whether and how to strengthen unity of effort for the full scope of defensive operations within the United States and beyond.

Secretary of homeland security Kirstjen Nielsen has called for the adoption of a "collective defense" posture that might include such expanded partnerships. Under the collective defense model, industry and government would collaborate to act on threat indicators and "respond more quickly and effectively to incidents."<sup>305</sup> The most familiar realm of operational collaboration lies in government support to help utilities detect, characterize, and eradicate malware on their systems. DHS is strengthening the National Cybersecurity and Communications Integration Center's ability to provide such assistance.<sup>306</sup> State National Guard organizations can also support post-cyber attack power restoration within the larger context of the industry's Cyber Mutual Assistance system.<sup>307</sup> However, in a cyber strike against the

United States, DOD will require many of these same guard personnel to protect the department's networks, conduct cyber operations against the attacker, and carry out other federal missions.<sup>308</sup> Power companies and government agencies will need to continue clarifying whether and how specific National Guard assets can help meet utility requests for assistance; existing doctrine and procedures for providing defense support to civil authorities offer a solid basis to advance those discussions.

In contrast, coordinating industry grid protection measures with government operations to suppress attacks would extend collective defense into uncharted territory. The command vision for US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, offers a starting point to examine how engaging against malicious cyber actors might help protect utilities. The document states that the United States must "increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage." To do so, DOD "is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems."<sup>309</sup>

Forward defense operations could respond to and help counter adversary efforts to implant malware on utility networks. Should such operations also help power companies protect their systems if the president declares that an attack is imminent? As senator Mike Rounds frames the question: "If someone is going to shoot an arrow at you, do you shoot the archer before he shoots the arrow?"<sup>310</sup>

US Cyber Command's vision statement does not directly address this possibility. However, each phase of grid security emergencies will likely offer

<sup>304</sup> GWU, *Into the Gray Zone*, 25.

<sup>305</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>306</sup> Marks, "DHS Stands Up New Cyber Risk Center."

<sup>307</sup> Crowe, "National Guard Preparing"; and Puryear, "91st Cyber Brigade Activated."

<sup>308</sup> DOD, *Cyber Strategy*, 4.

<sup>309</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 4–5.

<sup>310</sup> Bordelon, "Rounds Is Ready."

a different mix of risks and rewards for combining domestic and forward defense operations. For example, if the president determines that an attack on the grid is imminent, the secretary might issue orders for conservative operations to bolster grid defenses at the same moment that forward defense operations disrupted enemy cyber infrastructure poised to launch the strike. But assessments that an attack is imminent may turn out to be wrong. No-regrets orders for conservative operations are valuable precisely because using them will entail few consequences if warning indicators turn out to be false. Preattack forward defense operations could start a cyberwar that might not otherwise have occurred.

The United States can avoid such risks by waiting until attacks on the grid are under way before striking the enemy's offensive infrastructure. However, developing the technical capabilities to identify and disrupt the cyber infrastructure being used in an attack could prove challenging. Moreover, it is not clear whether integrating plans for home and away operations would offer significant benefits, as opposed to relying on utilities and government agencies to conduct those two types of operations independently.

US Cyber Command has opened the door to building new types of partnerships with the electricity subsector. The command has called for measures to "deepen and operationalize" collaboration between the private sector, the armed services, and other command partners.<sup>311</sup> As those efforts go forward with the electricity subsector and DOE, exploring options for collective defense (and clarifying the dangers they might present) should be a prime focus for analysis.

### **Maximizing Industry Contributions to Cyber Deterrence by Denial**

The *National Security Strategy* emphasizes that rather than rely on threats of cost imposition alone

to deter enemy attacks, the United States will also strengthen deterrence by denial. This report has examined how grid security emergency orders and implementation plans can raise adversaries' doubts as to whether they can achieve their objectives. But strengthening this form of deterrence will also entail underlying challenges.

Many cybersecurity analysts believe that offensive cyber capabilities are vastly stronger than defenses against them, and that this preeminence creates destabilizing incentives for adversaries to strike first when conflicts loom.<sup>312</sup> Unless measures to strengthen grid resilience can help weaken the dominance of offense over defense in the cyber realm, deterrence by denial will remain difficult to accomplish against highly capable adversaries.

However, today's offensive dominance stems in part from historical factors that are rapidly changing. The interconnected grid evolved decades ago when no cyber threat existed to drive protective measures. Moreover, as utilities began incorporating computer-assisted controls, sensors, and operating technology systems, few of these companies accounted for the risk that cyber threats to their systems would escalate so rapidly. As noted in this report, utilities are advancing a wide array of technical initiatives and fallback operational plans to counter and (ideally) stay ahead of adversaries' capabilities. In addition, regulatory bodies across the nation are increasingly willing to enable companies to recover costs for cyber resilience.

The current preeminence of offense over defense also reflects organizational factors. Rebecca Slayton has found that historically, "the success of offense is largely the result of a poorly managed defense."<sup>313</sup> The skills of the individuals employing cyber weapons and defensive tools, and the effectiveness with which

<sup>311</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 8.

<sup>312</sup> For a review of this "offense-dominant" literature, and the smaller set of works opposing it, see Slayton, "What Is the Cyber Offense-Defense Balance?," 72.

<sup>313</sup> Slayton, "What Is the Cyber Offense-Defense Balance?," 87.



these practitioners are managed and organized, have an enormous impact on the outcome of cyber engagements. Slayton notes that the importance of organization for cyber defense is implicit in discussions of the need for better public-private partnerships and information sharing. What has been missing, however, are efforts to make such partnerships *operational* and create unity of effort in government-industry defense actions when adversaries strike. That is precisely the gap that DOE and its industry partners can fill by developing grid security emergency orders and advancing all of the other collaborative initiatives necessary to make those orders effective.

Improved partnerships and technical capabilities to protect the grid cannot by themselves make defense preeminent. To further rebalance offense and defense in cyberspace, resilience initiatives will be necessary across all critical infrastructure sectors, as well as a host of other measures to facilitate the command, control, and coordination of public-private defensive operations. But building preparedness for grid security emergencies will be vital for that broader effort. Moreover, establishing defensive primacy is not necessary to facilitate deterrence by denial. As defined by the *National Security Strategy*, deterrence by denial functions by creating doubt in our adversaries that they can achieve their objectives.<sup>314</sup> DOE and its partners should develop grid security emergency orders that (perhaps in conjunction with forward defense operations) can make adversaries less likely to attack, even if defensive dominance remains out of reach.

Strengthening grid resilience can also support the broader reassessment of the US deterrence posture that is now under way. Robert Strayer, the State Department's deputy assistant secretary for cyber and international communications and information policy, notes that the increasing severity of threats to

US infrastructure is forcing "an evolution in the US government's thinking about how to deter malicious cyber actors."<sup>315</sup> In conventional warfare, deterrence by denial functions by making it physically difficult for adversaries to achieve their objectives and by raising enemy forces' costs of taking their targets.<sup>316</sup> Cyberwarfare will not entail the same sorts of attrition of enemy forces that occurs in battles with tanks, fighter aircraft, and other conventional weapons. The Trump and Obama administrations have redefined deterrence by denial to better fit the characteristics of cyberspace. The unique features of cyber conflict will require continued rethinking of how the United States can strengthen deterrence in the years to come. As utilities and government agencies build resilience for grid security emergencies, new opportunities will emerge to influence adversaries' perceived costs and benefits of attack. The United States should continue to refine its deterrence posture to capitalize on these improvements.

### Escaping the "Glass House" Syndrome

The president may need the ability to use cyber weapons against foreign targets to help resolve crises on terms favorable to the United States. The *DOD Cyber Strategy* (April 2015) states that:

There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an

<sup>314</sup> White House, *National Security Strategy*, 13.

<sup>315</sup> Smith, "U.S. Officials Push New Penalties."

<sup>316</sup> For definitions of classic deterrence by denial derived from conventional warfare, see Gerson, "Conventional Deterrence"; and Mitchell, "The Case for Deterrence by Denial." For an analysis of how that definition differs from that used by the Trump administration, see Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy."



ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests.<sup>317</sup>

However, any such operations against an adversary's cyber infrastructure would risk retaliatory strikes against the United States—including, potentially, attacks on the grid. Senator Thom Tillis (R-NC), a member of the Senate Armed Service Committee, emphasizes that the United States is living in “a big glass house.”<sup>318</sup> If US infrastructure owners and operators cannot defend their systems against attack, the president may be reluctant to use cyber weapons abroad, even if doing so might otherwise offer enormous benefits for conflict termination. In short: US leaders may be self-deterred from taking actions that they may need to employ. Developing emergency orders and implementation plans to protect grid reliability could reduce these glass house constraints and widen the range of options available for the president to protect US interests.

Improving grid defenses could also help strengthen the credibility of US commitments to defend key allies. Former US defense and intelligence officials have proposed that the United States and other high-cyber-capability NATO allies provide extended deterrence against cyber attacks for less capable alliance members.<sup>319</sup> But glass house concerns would call into question the credibility such commitments. Measures to strengthen grid resilience could help convince adversaries that the United States is willing to help allies respond to cyber attacks on their infrastructure.

Yet, nothing requires the United States to respond to such attacks with cyber weapons alone. On the contrary: the *National Security Strategy* and other policy documents leave open the possibility that

if cyber attacks at home or abroad are sufficiently severe, the United States will respond with conventional or even nuclear weapons. James Lewis notes that “opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return,” and will surely weigh that risk given “the immense capacity of the United States to inflict punishment” on attackers.<sup>320</sup> Emergency orders to protect the flow of power to defense installations can and should reinforce the certainty of that punishment.

But any first use of cyber weapons by the United States would entail escalatory dangers as well. If the United States were to initiate the use of destructive cyber weapons to defend US allies and interests, potential adversaries such as Russia could respond with conventional or nuclear forces. Moreover, conflicts that begin with the large-scale use of cyber weapons could also spiral out of control in ways that neither side desires or anticipates.<sup>321</sup> These escalatory risks must be in the forefront of calculations on whether and how to engage in cyber warfare. Indeed, as government agencies partner with power companies to build resilience for grid security emergencies, deterring such conflicts and reducing the likelihood of cyberwarfare should always be our prime objective.

<sup>317</sup> DOD, *Cyber Strategy*, 5.

<sup>318</sup> Schwartz, “Sen. Tillis: We Are Living in a Glass House.” For additional analysis of the glass house syndrome and its effects on constraining US options, see Miller, “Cyber Deterrence”; and Rosenbach, “Living in a Glass House.”

<sup>319</sup> Kramer, Butler, and Lotrionte, *Cyber, Extended Deterrence, and NATO*, 1.

<sup>320</sup> Lewis, *Rethinking Cybersecurity*, 9, 29. The author also argues that even if attacks on the grid occur, they would be unlikely to achieve the strategic effects that adversaries will seek, further reducing the likelihood of such attacks (see pp. 21 and 24–26).

<sup>321</sup> Danzig, *Surviving on a Diet of Poisoned Fruit*, 25; Lin, “Escalation Dynamics,” 52; and Miller and Fontaine, *A New Era*, 18–20.

## Bibliography

- 6 U.S.C. § 124l. <https://www.law.cornell.edu/uscode/text/6/124l>.
- 15 U.S.C. § 3361. <https://www.law.cornell.edu/uscode/text/15/3361>.
- 15 U.S.C. § 3363. <https://www.law.cornell.edu/uscode/text/15/3363>.
- 15 U.S.C. § 3364. <https://www.law.cornell.edu/uscode/text/15/3364>.
- 16 U.S.C. § 824a. <https://www.law.cornell.edu/uscode/text/16/824a>.
- 16 U.S.C. § 824o. <https://www.law.cornell.edu/uscode/text/16/824o>.
- 16 U.S.C. § 824o–1. <https://www.law.cornell.edu/uscode/text/16/824o–1>.
- 18 CFR 388.113. <https://www.law.cornell.edu/cfr/text/18/388.113>.
- 47 U.S.C. § 606. <https://www.law.cornell.edu/uscode/text/47/606>.
- 50 U.S.C. Appendix §2071(c). <https://law.justia.com/codes/us/2001/title50/app/defensepr/sec2071/>.
- “About Alerts.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx>.
- “About NERC.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/AboutNERC/Pages/default.aspx>.
- “About NSTAC.” DOS (US Department of State). Last published June 20, 2016. <https://www.dhs.gov/about-nstac>.
- “About 60% of the U.S. Electric Power Supply Is Managed by RTOs.” US Energy Information Administration. April 4, 2011. <https://www.eia.gov/todayinenergy/detail.php?id=790>.
- “Alert (ICS-ALERT-14-281-01E): Ongoing Sophisticated Malware Campaign Compromising ICS (Update E).” ICS-CERT. Originally released December 10, 2014, last revised December 9, 2016. <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.
- “Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure.” ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). February 25, 2016. <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.
- “Alert (TA17-163A): CrashOverride Malware.” US-CERT (US Computer Emergency Readiness Team). June 12, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-163A>.
- “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). October 20, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-293A>.
- “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). March 15, 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.

- ASD(EI&E) (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment). *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*. Washington, DC: DOD, July 2017. <https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf>.
- Assante, Michael, and Robert M. Lee. *The Industrial Control System Cyber Kill Chain*. Bethesda, MD: SANS Institute, October 2015. <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.
- “Automated Indicator Sharing (AIS).” US-CERT (US Computer Emergency Readiness Team). n.d. <https://www.us-cert.gov/ais>.
- Banham, Russ. “DDoS Attacks Evolve to Conscript Devices onto the IoT.” *Forbes*, February 4, 2018. <https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#4b5a43a86aaa>.
- Barnes, Julian E. “‘Warning Lights Are Blinking Red,’ Top Intelligence Officer Says of Russian Attacks.” *New York Times*, July 13, 2018. <https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html>.
- Blue Ribbon Study Panel on Biodefense (Hudson Institute). *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts—A Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*. Washington, DC: Hudson Institute, October 2015. <http://www.biodefensestudy.org/a-national-blueprint-for-biodefense>.
- Bordelon, Brendan. “Rounds Is Ready to Lead New Senate Cybersecurity Subcommittee.” *Morning Consult*, February 1, 2017. <https://morningconsult.com/2017/02/01/rounds-ready-lead-new-senate-cybersecurity-subcommittee/>.
- Brown, Jared T., and Daniel H. Else. *The Defense Production Act of 1950: History, Authorities, and Reauthorization*. Washington, DC: Congressional Research Service, July 28, 2014. <https://fas.org/sgp/crs/natsec/R43118.pdf>.
- “The Canada-U.S. Defence Relationship.” Department of National Defence and the Canadian Armed Forces. December 4, 2014, last modified February 10, 2015. <http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s>.
- Cherepanov, Anton, and Robert Lipovsky. “Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet.” *WeLiveSecurity* (ESET Blog), June 12, 2017. <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.
- “Compendium of U.S.-Canada Emergency Management Assistance Mechanisms.” Public Safety Canada. October 2016, last modified March 28, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cmpndm-ntdstts-cnd-2016/index-en.aspx>.
- “Compliance - Québec.” Northeast Power Coordinating Council. n.d. <https://www.npcc.org/Compliance/Quebec/Forms/Public%20List.aspx>.
- Cowan, Gerrard. “Locked Shields 2018 Practises for Large-Scale Cyber Incident.” *Jane’s 360*, April 29, 2018. <http://www.janes.com/article/79652/locked-shields-2018-practises-for-large-scale-cyber-incident>.

- Crowe, Greg. "National Guard Preparing to Defend Cyberspace for States." *Federal News Radio*, April 16, 2018. <https://federalnewsradio.com/cyber-exposure/2018/04/national-guard-preparing-to-defend-cyberspace-for-states/>.
- "Cybersecurity." American Gas Association. n.d. <https://www.aga.org/safety/security/cybersecurity/>.
- "The Cyber Threat Framework." ODNI (Office of the Director of National Intelligence). n.d. <https://www.dni.gov/index.php/cyber-threat-framework>.
- Danzig, Richard. *Catastrophic Bioterrorism—What Is to Be Done?* Washington, DC: Center for Technology and National Security Policy, August 2003. [http://www.response-analytics.org/images/Danzig\\_Bioterror\\_Paper.pdf](http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf).
- . *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Washington, DC: Center for a New American Security, July 2014. [https://s3.amazonaws.com/files.cnas.org/documents/CNAS\\_PoisonedFruit\\_Danzig.pdf](https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf).
- Defense Science Board. *Task Force on Cyber Deterrence*. Washington, DC: DOD, February 2017. [https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport\\_02-28-17\\_Final.pdf](https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf).
- DHS (US Department of Homeland Security). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: DHS, December 17, 2003. <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- . *National Cyber Incident Response Plan*. Washington, DC: DHS, December 2016. [https://www.us-cert.gov/sites/default/files/ncirp/National\\_Cyber\\_Incident\\_Response\\_Plan.pdf](https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf).
- . *National Response Framework*. 3rd ed. Washington, DC: DHS, June 2016. [https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National\\_Response\\_Framework3rd.pdf](https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf).
- . *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS, 2013. <https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf>.
- . *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage*. Washington, DC: DHS, June 2017. <https://www.fema.gov/media-library/assets/documents/154058>.
- . *Strategy for Protecting and Preparing the Homeland against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*. Washington, DC: DHS, forthcoming.
- . *U.S. Department of Homeland Security Cybersecurity Strategy*. Washington, DC: DHS, May, 15, 2018. [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf).
- DiSavino, Scott, and David Sheppard. "ConEd Cuts Power to Part of Lower Manhattan Due to Sandy." *Reuters*, October 29, 2012. <https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030>.

- DOD (US Department of Defense). *Department of Defense Manual 3020.45*. Washington, DC: DOD, last updated May 23, 2017. <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>.
- . *DoD Cybersecurity Discipline Implementation Plan*. Washington, DC: DOD, amended February 2016. <http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf>.
- . *DOD Cyber Strategy*. Washington, DC: DOD, April 2015. [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).
- . *DoD Directive 3020.40: Mission Assurance (MA)*. Washington, DC: DOD, November 29, 2016. [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).
- . *Mission Assurance Strategy*. Washington, DC: DOD, April 2012. [http://policy.defense.gov/Portals/11/Documents/MA\\_Strategy\\_Final\\_7May12.pdf](http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf).
- DOE (US Department of Energy). “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40).” *Federal Register* 83, no. 7 (2018): 1176. <https://www.federalregister.gov/documents/2018/01/10/2018-00259/grid-security-emergency-orders-procedures-for-issuance>.
- . *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. Version 1.1. Washington, DC: DOE, February 2014. <https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf>.
- . *Electromagnetic Pulse Resilience Action Plan*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf>.
- . “Energy Priorities and Allocations System Regulations (RIN 1901–AB28).” *Federal Register* 76, no. 111 (2011): 33615. <https://www.gpo.gov/fdsys/pkg/FR-2011-06-09/pdf/2011-14282.pdf>.
- . *Multiyear Plan for Energy Sector Cybersecurity*. Washington, DC: DOE, March 2018. [https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20\\_0.pdf](https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf).
- . *Quadrennial Energy Review—Transforming the Nation’s Electricity System: The Second Installment of the QER*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>.
- . *Staff Report to the Secretary on Electricity Markets and Reliability*. Washington, DC: DOE, August 2017. [https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability\\_0.pdf](https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability_0.pdf).
- . *Strategic Transformer Reserve: Report to Congress*. Washington, DC: DOE, March 2017. <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.
- “DOE’s Use of Federal Power Act Emergency Authority.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use>.



- DOS (US Department of State). *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. Washington, DC: DOS, May 31, 2018. <https://www.state.gov/documents/organization/282253.pdf>.
- Dougherty, Jon. “Biggest U.S. Power Grid Operator Suffers Thousands of Attempted Cyber Attacks per Month.” *Forward Observer*, August 28, 2017. <https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/>.
- Douris, Constance. “DARPA Research Leads Grid Security Solutions.” *The Buzz* (blog), *National Interest*, January 12, 2017. <http://nationalinterest.org/blog/the-buzz/darpa-research-leads-grid-security-solutions-19044>.
- Dragos, Inc. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. Hanover, MD: Dragos, June 13, 2017. <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>.
- EEI (Edison Electric Institute). “Comments of the Edison Electric Institute.” In *Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*. February 6, 2017.
- . *Understanding the Electric Power Industry’s Response and Restoration Process*. Washington, DC: EEI, October 2016. [http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA\\_101FINAL.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf).
- EIS Council (Electric Infrastructure Security Council). *E-PRO Handbook II: Volume 1—Fuel*. Washington, DC: EIS Council, 2016. [https://www.eiscouncil.org/App\\_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf](https://www.eiscouncil.org/App_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf).
- . *E-PRO Handbook III: Black Sky Cross-Sector Coordination and Communication*. Washington, DC: EIS Council, June 2018. [https://www.eiscouncil.org/EPRO\\_Books.aspx](https://www.eiscouncil.org/EPRO_Books.aspx).
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS-ICS. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Washington, DC: NERC, March 2016. [https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_18Mar2016.pdf](https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf).
- “Electricity Information Sharing and Analysis Center.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.
- “Electric Power Transmission Reliability Standards Compliance Monitoring and Enforcement.” Régie de l’énergie Québec. n.d. <http://www.regie-energie.qc.ca/en/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html>.
- “Emergency Communications.” DHS (US Department of Homeland Security). Last published June 26, 2018. <https://www.dhs.gov/topic/emergency-communications>.
- Energy Policy Act of 2005. Public Law 109-58. *U.S. Statutes at Large* 119 (2005): 942–943. <https://www.gpo.gov/fdsys/pkg/STATUTE-119/pdf/STATUTE-119.pdf>.
- “Energy Sector Cybersecurity Preparedness.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

- EPRI (Electric Power Research Institute). *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research*. Report 3002000796. Palo Alto, CA: EPRI, December 2013. <https://publicdownload.epri.com/PublicDownload.svc/product=000000003002000796/type=Product>.
- . *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs*. Report 3002008999. Palo Alto, CA: EPRI, September 2016. <https://www.epri.com/#/pages/product/000000003002008999/?lang=en>.
- ESCC (Electricity Subsector Coordinating Council). *Electricity Sub-Sector Coordinating Council Charter*. Washington, DC: DHS, August 5, 2013. <https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf>.
- “ESCC: Electricity Subsector Coordinating Council.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.
- “The ESCC’s Cyber Mutual Assistance Program.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1>.
- FEMA (US Federal Emergency Management Agency). *2017 Hurricane Season FEMA After-Action Report*. Washington, DC: FEMA, July 12, 2018. <https://www.fema.gov/media-library/assets/documents/167249>.
- FERC (Federal Energy Regulatory Commission). *Cyber Security Incident Reporting Reliability Standards*. 161 FERC ¶ 61,291. December 21, 2017. <https://www.ferc.gov/whats-new/comm-meet/2017/122117/E-1.pdf>.
- . *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies, Statement of Policy*. 96 FERC ¶ 61,299. September 14, 2011.
- . *Grid Resilience in Regional Transmission Organizations and Independent System Operators*. 162 FERC ¶ 61,256. 2018. <https://www.ferc.gov/CalendarFiles/20180320102618-AD18-7-000.pdf>.
- . *Order Authorizing Acquisition and Disposition of Jurisdictional Facilities*. 163 FERC ¶ 61,005. April 3, 2018. <https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf>.
- . *Order Granting Approvals in Connection with the Dissolution of the Southwest Power Pool Regional Entity*. 163 FERC ¶ 61,094. May 4, 2018. <https://www.ferc.gov/CalendarFiles/20180504141902-RR18-3-000.pdf>.
- . *Policy Statement on Matters Related to Bulk Power System Reliability*. 107 FERC ¶ 61,052. April 19, 2004. <https://www.ferc.gov/whats-new/comm-meet/041404/E-6.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833. 157 FERC ¶ 61,123. November 17, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-4.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833-A. 163 FERC ¶ 61,125. May 17, 2018. <https://www.ferc.gov/whats-new/comm-meet/2018/051718/E-2.pdf>.

- . *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*. 156 FERC ¶ 61,215. September 22, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/092216/E-4.pdf>.
- . *Revision to Electric Reliability Organization Definition of Bulk Electric System*. Order No. 743. 133 FERC ¶ 61,150. November 18, 2010. <https://www.ferc.gov/whats-new/comm-meet/2010/111810/E-2.pdf>.
- . *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*. Order No. 773-A. 143 FERC ¶ 61,053. April 18, 2013. <https://www.ferc.gov/whats-new/comm-meet/2013/041813/E-9.pdf>.
- FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation). *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*. Washington, DC: FERC, January 2016. <https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Further Joint Study Report: Planning Restoration Absent SCADA or EMS (PRASE)*. Washington, DC: FERC, June 2017. <https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Recommended Study: Blackstart Resources Availability (BRAv)*. Washington, DC: FERC, May 2018. <https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf>.
- Fischerkeller, Michael P., and Richard J. Harknett. “Deterrence Is Not a Credible Strategy for Cyberspace.” *Orbis* 61, no. 3 (2017): 381–393. <https://www.sciencedirect.com/science/article/pii/S0030438717300431>.
- Fixing America’s Surface Transportation Act, Public Law 114-94. *U.S. Statutes at Large* 129 (2015): 1773–1774. <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.
- Frankel, Alison. “Can Customers Sue Power Companies for Outages? Yes, but It’s Hard to Win.” *Reuters* (blog), November 9, 2012. <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>.
- Galloway, T. J., Sr. “Advancing Reliability and Resilience of the Grid.” Comments presented at the FERC Reliability Technical Conference, Washington, DC, July 31, 2018. <https://www.ferc.gov/CalendarFiles/20180731084251-Galloway,%20North%20American%20Transmission%20Forum.pdf>.
- Gerson, Michael S. “Conventional Deterrence in the Second Nuclear Age.” *Parameters* 39 (Autumn 2009): 32–48. <https://ssi.armywarcollege.edu/pubs/parameters/articles/09autumn/gerson.pdf>.
- Governments of the US and Canada. *Joint United States-Canada Electric Grid Security and Resilience Strategy*. Washington, DC: The White House, December 2016. [https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint\\_US\\_Canada\\_Grid\\_Strategy\\_06Dec2016.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf).
- GWU (George Washington University) Center for Cyber and Homeland Security. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: GWU, October 2016. <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf>.
- Healy, Jason. *The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities*. SSRN, June 2016. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2836206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206).

- Homeland Security Advisory Council. *Final Report of the Cybersecurity Subcommittee: Part I—Incident Response*. Washington, DC: DOS, June 2016. <https://www.hsd.org/?view&did=794271>.
- ICF. *Assessment of Large Power Transformer Risk Mitigation Strategies*. Fairfax, VA: ICF, October 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf>.
- . *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. Fairfax, VA: ICF, June 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>.
- “Increasing Electricity Cooperation in North America.” DOE (US Department of Energy). January 11, 2017. <https://www.energy.gov/policy/articles/increasing-electricity-cooperation-north-america>.
- INL (Idaho National Laboratory). *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*. Idaho Falls, IN: INL, January 2016. <https://inldigitallibrary.inl.gov/sites/STI/STI/INL-EXT-15-35582.pdf>.
- ISO-NE (ISO New England). *Operational Fuel-Security Analysis*. Holyoke, MA: ISO-NE, January 17, 2018. [https://www.iso-ne.com/static-assets/documents/2018/01/20180117\\_operational\\_fuel-security\\_analysis.pdf](https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf).
- . “Response of ISO New England Inc.” *Response to Grid Resilience in Regional Transmission Organization and Independent System Operators* (AD18-7-000). March 9, 2018. [https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7\\_iso\\_response\\_to\\_grid\\_resilience.pdf](https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7_iso_response_to_grid_resilience.pdf).
- Jenkins, Brian Michael. “Countering al-Qaeda: The Next Phase in the War.” *The RAND Blog*, September 8, 2002. <https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html>.
- Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*. Joint Publication 1. Washington, DC: Joint Chiefs of Staff, July 12, 2017. [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1\\_ch1.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf).
- Joint Commenters. “Comments of American Public Power Association, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group.” In *Response to RIN 1901-AB40*. February 23, 2017. <http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf>.
- Kaften, Cheryl. “DoD Tests Energy Continuity with ‘Islanded’ Microgrid.” *Energy Manager Today*, April 5, 2017. <https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/>.
- Kappenman, John. *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*. Goleta, CA: Metatech, January 2010. [https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc\\_meta-r-319.pdf](https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf).
- “Key Players.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>.
- Kissane, Carolyn, and Emily Medina. “Energy Aftershocks in Store after Seismic Mexican Election.” *The Hill*, July 3, 2018. <http://thehill.com/opinion/energy-environment/395383-energy-aftershocks-in-store-after-seismic-mexican-election>.



- Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte. *Cyber, Extended Deterrence, and NATO*. Washington, DC: Atlantic Council, May 2016. [http://www.atlanticcouncil.org/images/publications/Cyber\\_Extended\\_Deterrence\\_and\\_NATO\\_web\\_0526.pdf](http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf).
- Lawrence, Bill, Charlotte de Seibert, and Philip Daigle. "E-ISAC Update." Presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, FL, March 6–7, 2018. <https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf>.
- Lazar, Jim. *Electricity Regulation in the US: A Guide*. 2nd ed. Montpelier, VT: Regulatory Assistance Project, June 2016. <http://www.raponline.org/wp-content/uploads/2016/07/rap-lazar-electricity-regulation-US-june-2016.pdf>.
- Lewis, James A. "North Korea and Cyber Catastrophe—Don't Hold Your Breath." *38 North*, January 12, 2018. <http://www.38north.org/2018/01/jalewis011218/>.
- . *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Washington, DC: CSIS, January 2018. [http://espas.eu/orbis/sites/default/files/generated/document/en/180108\\_Lewis\\_ReconsideringCybersecurity\\_Web.pdf](http://espas.eu/orbis/sites/default/files/generated/document/en/180108_Lewis_ReconsideringCybersecurity_Web.pdf).
- Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. [http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06\\_Issue-3/Fall12.pdf](http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-3/Fall12.pdf).
- Lucas, Todd. "Conservative Operations." Presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, CO, September 18–19, 2013. <http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf>.
- Lynch, Justin. "How the Russian Government Allegedly Attacks the American Electric Grid." *Fifth Domain*, July 24, 2018. <https://www.fifthdomain.com/critical-infrastructure/2018/07/24/how-the-russian-government-attacks-the-american-electric-grid/>.
- Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (Sept./Oct. 2010). <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.
- "Maritime Forces Pacific." Royal Canadian Navy. Last modified November 24, 2016. <http://www.navy-marine.forces.gc.ca/en/about/structure-marpac-home.page>.
- Marks, Joseph. "DHS Stands up New Cyber Risk Center to Protect High-Value Targets." *Nextgov*, July 31, 2018. <https://www.nextgov.com/cybersecurity/2018/07/dhs-stands-new-cyber-risk-center-protect-high-value-targets/150179/>.
- Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn. *Power Begins at Home: Assured Energy for U.S. Military Bases*. Reston, VA: Noblis, January 12, 2017. [http://www.pewtrusts.org/~media/assets/2017/01/ce\\_power\\_begins\\_at\\_home\\_assured\\_energy\\_for\\_us\\_military\\_bases.pdf](http://www.pewtrusts.org/~media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf).
- McElwee, Steven. "Probabilistic Cluster Ensemble Evaluation for Unsupervised Intrusion Detection." Unpublished thesis, Nova Southeastern University, forthcoming.



- McElwee, Steven, Jeffrey Heaton, James Fraley, and James Cannady. "Deep Learning for Prioritizing and Responding to Intrusion Detection Alerts." In *2017 IEEE Military Communications Conference Proceedings*. Piscataway, NJ: IEEE, 2017. <https://ieeexplore.ieee.org/document/8170757/>.
- McGhee, Michael. "EEI Executive Advisory Committee." Slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017. [http://www.asaie.army.mil/Public/ES/oei/docs/EEI\\_Exec-Committee.pdf](http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf).
- Miller, James N. "Cyber Deterrence Cannot Be One Size Fits All." *Cipher Brief*, August 3, 2017. [https://www.thecipherbrief.com/column\\_article/cyber-deterrence-cannot-be-one-size-fits-all-1092](https://www.thecipherbrief.com/column_article/cyber-deterrence-cannot-be-one-size-fits-all-1092).
- Miller, James N., and James R. Gosler. "Memorandum for the Chairman, Defense Science Board" (preamble). In *Task Force on Cyber Deterrence*. Washington, DC: Defense Science Board, February 2017. <http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>.
- Miller, James N., Jr., and Richard Fontaine. *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict*. Washington, DC: CNAS, September 2017. <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Project Pathways-Finalb.pdf?mtime=20170918101505>.
- Miller, Rich. "Con Edison Shuts off Power in Lower Manhattan." *DataCenter Knowledge*, October 29, 2012. <http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutdown>.
- MISO (Midcontinent Independent System Operator). *Geomagnetic Disturbance Operations Plan*. SO-P-AOP-01 Rev: 1. Carmel, IN: MISO, June 9, 2017. [https://old.misoenergy.org/\\_layouts/miso/ecm/redirect.aspx?id=252214](https://old.misoenergy.org/_layouts/miso/ecm/redirect.aspx?id=252214).
- . "MISO January 17–18 Maximum Generation Event Overview." Slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018. <https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf>.
- Mitchell, A. Weiss. "The Case for Deterrence by Denial." *American Interest*, August 12, 2015. <https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/>.
- "M-1 Reserve Margin." NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.
- Murauskaite, Egle. "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment." *38 North*, September 12, 2014. <http://www.38north.org/2014/09/emurauskaite091214/>.
- Nakashima, Ellen. "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks." *Washington Post*, July 8, 2017. [https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47\\_story.html](https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html).
- NARUC (National Association of Regulatory Utility Commissioners). *Cybersecurity: A Primer for State Utility Regulators*. Version 3.0. Washington, DC: NARUC, January 2017. <https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F>.

- . *Resolution on Physical Security*. Washington, DC: NARUC, July 16, 2014. <https://pubs.naruc.org/pub.cfm?id=53A0CAA5-2354-D714-5127-E0C411BAD460>.
- NASEO (National Association of State Energy Officials). “Comments of the National Association of State Energy Officials.” In *Response to RIN 1901–AB40*. [https://www.naseo.org/Data/Sites/1/naseo-comments\\_rin-1901%E2%80%93ab40.pdf](https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901%E2%80%93ab40.pdf).
- NATF (North American Transmission Forum). *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—A Spare Tire Approach*. Charlotte, NC: NATF, 2017. <http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf>.
- . *North American Transmission Forum External Newsletter*. Charlotte, NC: NATF, January 2018. <https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf>.
- National Defense Authorization Act for Fiscal Year 2017. Public Law 114-328. *U.S. Statutes at Large* 130 (2016): 2685–2687. <https://www.gpo.gov/fdsys/pkg/PLAW-114publ328/pdf/PLAW-114publ328.pdf>.
- NERC (North American Electric Reliability Corporation). *BAL-002-2(i)—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. Washington, DC: NERC, January 1, 2018. [https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2\(i\).pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2(i).pdf).
- . *CIP-014-2—Physical Security*. Washington, DC: NERC, October 2, 2015. <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.
- . *EOP-010-1—Geomagnetic Disturbance Operations*. Washington, DC: NERC, June 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States).
- . *EOP-011-1—Emergency Operations*. Washington, DC: NERC, April 1, 2017. [https://www.nerc.com/\\_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).
- . *Glossary of Terms Used in NERC Reliability Standards*. Washington, DC: NERC, last updated July 3, 2018. [https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary\\_of\\_Terms.pdf](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf).
- . *Grid Security Exercise: GridEx III Report*. Atlanta, GA: NERC, March 2016. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.
- . *Grid Security Exercise GridEx IV: Lessons Learned*. Atlanta, GA: NERC, March 28, 2018. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf>.
- . *History of NERC*. Washington, DC: NERC, August 2013. <http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf>.
- . *Hurricane Harvey Event Analysis Report*. Washington, DC: NERC, March 2018. [https://www.nerc.com/pa/rrm/ea/Hurricane\\_Harvey\\_EAR\\_DL/NERC\\_Hurricane\\_Harvey\\_EAR\\_20180309.pdf](https://www.nerc.com/pa/rrm/ea/Hurricane_Harvey_EAR_DL/NERC_Hurricane_Harvey_EAR_20180309.pdf).

- . “Informational Filing on the Definition of ‘Adequate Level of Reliability.’” Filing to the Federal Energy Regulatory Commission. May 10, 2013. [https://www.nerc.com/pa/Stand/Resources/Documents/Adequate\\_Level\\_of\\_Reliability\\_Definition\\_\(Informational\\_Filing\).pdf](https://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf).
- . *IRO-008-2—Reliability Coordinator Operational Analysis and Real-Time Assessments*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/IRO-008-2.pdf>.
- . *PRC-010-2—Under Voltage Load Shedding*. Washington, DC: NERC, April 2, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States).
- . *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*. Atlanta, GA: NERC, December 13, 2017. [https://www.nerc.com/comm/OC\\_Reliability\\_Guidelines\\_DL/Gas\\_and\\_Electrical\\_Operational\\_Coordination\\_Considerations\\_20171213.pdf](https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Gas_and_Electrical_Operational_Coordination_Considerations_20171213.pdf).
- . *Reliability Terminology*. Atlanta, GA: NERC, August 2013. <https://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf>.
- . *Short-Term Special Assessment: Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation*. Atlanta, GA: NERC, May 2016. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric\\_Final.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric_Final.pdf).
- . *Standard PRC-006-3—Automatic Underfrequency Load Shedding*. Washington, DC: NERC, October 1, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States).
- . *Technical Report Supporting Definition of Adequate Level of Reliability*. Washington, DC: NERC, March 26, 2013. <https://www.nerc.com/comm/Other/Pages/Adequate%20Level%20of%20Reliability%20Task%20Force%20ALRTF.aspx>.
- . *TOP-001-3—Transmission Operations*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-001-3.pdf>.
- . *TPL-007-1—Transmission System Planned Performance for Geomagnetic Disturbance Events*. Washington, DC: NERC, December 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States).
- . *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power Phase II: A Vulnerability and Scenario Assessment for the North American Bulk Power System*. Atlanta, GA: NERC, May 2013. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC\\_PhaseII\\_FINAL.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf).
- . *2016 Long-Term Reliability Assessment*. Atlanta, GA: NERC, December 2016. <https://www.nerc.com/pa/rapa/ra/reliability%20assessments%20dl/2016%20long-term%20reliability%20assessment.pdf>.
- . *VAR-001-4.2—Voltage and Reactive Control*. Washington, DC: NERC, September 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/VAR-001-4.2.pdf>.

- NERC (North American Electric Reliability Corporation) Steering Group. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* Princeton, NJ: NERC, July 13, 2014. [https://www.nerc.com/docs/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](https://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC (North American Electric Reliability Corporation) System Protection and Control Subcommittee. *Reliability Fundamentals of System Protection*. Princeton, NJ: NERC, December 2010. [https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals\\_Approved\\_20101208.pdf](https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals_Approved_20101208.pdf).
- NETL (National Energy Technology Laboratory). *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units—Volume I: The Critical Role of Thermal Units during Extreme Weather Events*. Washington, DC: DOE, March 13, 2018. <https://www.netl.doe.gov/research/energy-analysis/search-publications/vuedetails?id=2594>.
- Newman, Lily Hay. “Hacker Lexicon: What Is the Attribution Problem?” *Wired*, December 24, 2016. <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.
- NIAC (National Infrastructure Advisory Council). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. Washington, DC: NIAC, August 2017. <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>.
- Nielsen, Kirstjen M. “National Cybersecurity Summit Keynote Speech.” DHS (Department of Homeland Security). Released July 31, 2018. <https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech>.
- “NOAA Space Weather Scales.” NOAA. April 2011. <https://www.swpc.noaa.gov/sites/default/files/images/NOAAscales.pdf>.
- “North America.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/Canada.aspx>.
- “The North Atlantic Treaty.” North Atlantic Treaty Organization. April 4, 1949 (as amended). [https://www.nato.int/cps/ic/natohq/official\\_texts\\_17120.htm](https://www.nato.int/cps/ic/natohq/official_texts_17120.htm).
- Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016/2017): 44–71. [https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\\_a\\_00266](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266).
- Obama, Barack. *Executive Order—Assignment of National Security and Emergency Preparedness Communications Functions*. Washington, DC: The White House, July 6, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness->.
- . *Executive Order—Coordinating Efforts to Prepare the Nation for Space Weather Events*. Washington, DC: The White House, October 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events>.
- . *Executive Order—Improving Critical Infrastructure Cybersecurity*. Executive Order 13636. Washington, DC: The White House, February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.



- . *Executive Order—National Defense Resources Preparedness*. Washington, DC: The White House, March 16, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/03/16/executive-order-national-defense-resources-preparedness>.
- . *United States Cyber Incident Coordination*. Presidential Policy Directive 41. Washington, DC: The White House, July 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
- ODNI (Office of the Director of National Intelligence). *A Common Threat Framework: A Foundation for Communication*. McLean, VA: ODNI, January 26, 2018.
- Orenstein, Daniel G., and Lexi C. White. *Emergency Declaration Authorities across All States and D.C.* Edina, MN: Network for Public Health Law, June 16, 2015. [https://www.networkforphl.org/\\_asset/gxrdwm/Emergency-Declaration-Authorities.pdf](https://www.networkforphl.org/_asset/gxrdwm/Emergency-Declaration-Authorities.pdf).
- Paradise, Theodore J., et al. “ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance—RIN 1901–AB40.” Email to Jeffrey Baumgartner, US Department of Energy, February 6, 2017. [http://www.isorto.org/Documents/Report/20170206\\_Final\\_IRC-DOE\\_NOPR\\_Comments\\_re\\_Grid\\_Security\\_Emergency.pdf](http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf).
- Parfomak, Paul W. *Pipelines: Securing the Veins of the American Economy, Testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*. Washington, DC: Congressional Research Service, April 19, 2016. <http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf>.
- Parfomak, Paul W., Richard J. Campbell, Robert Pirog, Michael Ratner, Phillip Brown, John Frittelli, and Marc Humphries. *Cross-Border Energy Trade in North America: Present and Potential*. Washington, DC: Congressional Research Service, January 30, 2017. <https://fas.org/sgp/crs/misc/R44747.pdf>.
- Perry, Richard (US secretary of energy). Letter to the Federal Energy Regulatory Commission. September 28, 2017. <https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf>.
- Phillips, Tony. “Solar Shield—Protecting the North American Power Grid.” *NASA Science*, October 26, 2010. [https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\\_solarshield](https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield).
- PJM. “Comments and Responses of PJM Interconnection, L.L.C.” In *Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000). March 9, 2018. <http://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx>.
- . “Conservative Operations.” Training materials presented on January 27, 2015. <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.
- . *PJM Manual 13: Emergency Operations*. Rev. 65. Audubon, PA: PJM, January 1, 2018. <http://www.pjm.com/~/-/media/documents/manuals/m13.ashx>.



- Puryear, Cotton. "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade." *National Guard*, September 19, 2017. <http://www.nationalguard.mil/News/Article/1315685/91st-cyber-brigade-activated-as-army-national-guards-first-cyber-brigade/>.
- Reagan, Ronald. "The President's News Conference." August 12, 1986. Transcript. The American Presidency Project, Gerhard Peters and John T. Woolley. <http://www.presidency.ucsb.edu/ws/?pid=37733>.
- "Reliability Coordinators." NERC (North American Electric Reliability Corporation). As of June 1, 2015. <https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.
- "REMEDYS: Research Exploring Malware in Energy Delivery Systems." Cyber Resilient Energy Delivery Consortium. March 26, 2018. <https://cred-c.org/researchactivity/remedys-research-exploring-malware-energy-delivery-systems>.
- "The Role of Microgrids in Helping to Advance the Nation's Energy System." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/role-microgrids-helping>.
- "Roles and Responsibilities of Governments in Natural Resources." Natural Resources Canada. Last modified October 2, 2017. <http://www.nrcan.gc.ca/mining-materials/taxation/8882>.
- Rosenbach, Eric. "Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks." *Prepared Statement for the United States Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*. June 12, 2017. [https://www.foreign.senate.gov/imo/media/doc/061317\\_Rosenbach\\_Testimony.pdf](https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf).
- "Sandia's Grid Modernization Program Newsletter." Sandia National Laboratories. December 2017. <https://content.govdelivery.com/accounts/USDOESNLEC/bulletins/1c11ce6>.
- Schwartz, Ian. "Sen. Tillis: We Are Living in a Glass House Throwing Rocks Complaining about Election Interference." *RealClear Politics*, January 5, 2017. [https://www.realclearpolitics.com/video/2017/01/05/sen\\_tillis\\_we\\_are\\_living\\_in\\_a\\_glass\\_house\\_throwing\\_rocks\\_complaining\\_about\\_election\\_interference.html](https://www.realclearpolitics.com/video/2017/01/05/sen_tillis_we_are_living_in_a_glass_house_throwing_rocks_complaining_about_election_interference.html).
- "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response." DOE (Department of Energy). February 14, 2018. <https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency>.
- SERC. *Conservative Operations Guidelines*. Guide-800-101. Charlotte, NC: SERC, May 20, 2015. [https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines\\_rev-0-\(05-20-15\).pdf?sfvrsn=2](https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2).
- Severe Impact Resilience Task Force. *Severe Impact Resilience: Considerations and Recommendations*. Washington, DC: NERC, May 9, 2012. [https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF\\_Final\\_May\\_9\\_2012-Board\\_Accepted.pdf](https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf).

- Shelton, William L. "Threats to Space Assets and Implications for Homeland Security." *Written Testimony before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*. March 29, 2017. <http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf>.
- Sistrunk, Chris. "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)." *SANS Industrial Control Systems Security Blog*, January 8, 2016. <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>.
- Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (Winter 2016/17): 73–109. [https://www.mitpressjournals.org/doi/10.1162/ISEC\\_a\\_00267](https://www.mitpressjournals.org/doi/10.1162/ISEC_a_00267).
- Smith, Rebecca. "U.S. Officials Push New Penalties for Hackers of Electrical Grid." *Wall Street Journal*, August 5, 2018. <https://www.wsj.com/articles/u-s-officials-push-new-penalties-for-hackers-of-electrical-grid-1533492714>.
- Smith, Scott S. "Roles and Responsibilities for Defending the Nation from Cyber Attack." *Testimony Before the Senate Armed Services Committee*. October 19, 2017. <https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities>.
- Sobczak, Blake, Hannah Northey, and Peter Behr. "Cyber Raises Threat against America's Energy Backbone." *Energy Wire*, May 23, 2017. <https://www.eenews.net/stories/1060054924/>.
- Social Media Working Group for Emergency Services and Disaster Management. *Countering False Information on Social Media in Disasters and Emergencies*. Washington, DC: DHS, March 2018. [https://www.dhs.gov/sites/default/files/publications/SMWG\\_Countering-False-Info-Social-Media-Disasters-Emergencies\\_Mar2018-508.pdf](https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf).
- "Spare Transformers." EEI (Edison Electric Institute). n.d. <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.
- Stanley, Andrew J. *Mapping the U.S.-Canada Energy Relationship*. Washington, DC: CSIS, May 2018. [https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507\\_St Stanley\\_U.S.CanadaEnergy.pdf?fbWWhKl0BBuNMOeIRSolkNQ89Iij7iaz](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507_St Stanley_U.S.CanadaEnergy.pdf?fbWWhKl0BBuNMOeIRSolkNQ89Iij7iaz).
- "State and Local Energy Assurance Planning." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/energy-assurance/emergency-preparedness/state-and-local-energy-assurance-planning>.
- State of New Jersey Board of Public Utilities. *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196). March 18, 2016. <http://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf>.
- Stockton, Paul. On behalf of Exelon Corporation. *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*. Docket No. RM18-1-000. October 23, 2017.
- . "Thresholds and Criteria for Declaring Grid Security Emergencies." Study for the US Department of Energy. January 31, 2018.

- Sukumar, Arun M. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare* (blog), July 4, 2017. <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.
- "Transmission Equipment Ready When Needed." Grid Assurance. n.d. <http://www.gridassurance.com/equipment-subscribers/>.
- Trump, Donald. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Executive Order 13800. Washington, DC: The White House, May 11, 2017. <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
- Ucci, Daniele, Leonardo Aniello, and Roberto Baldoni. "Survey on the Usage of Machine Learning Techniques for Malware Analysis." *ACM Transactions on the Web* 1, no. 1 (October 2017): 1:1–1:34. <https://pdfs.semanticscholar.org/d310/47e426b8b5c2aa52108899a800bedd966f07.pdf>.
- "United States Mandatory Standards Subject to Enforcement." NERC. n.d. <https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States>.
- U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington, DC: DOE, April 2004. <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.
- US Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington, DC: US Cyber Command, released March 2018. <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>.
- Van Broekhoven, S. B., N. Judson, S. V. T. Nguyen, and W. D. Ross. *Microgrid Study: Energy Security for DoD Installations*. Technical Report 1164. Lexington, MA: MIT, June 2012. <https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf>.
- Vine, Doug. *Interconnected: Canadian and U.S. Electricity*. Arlington, VA: Center for Climate and Energy Solutions, March 2017. <https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf>.
- Walker, Bruce J. *Written Testimony before the U.S. Senate Committee on Energy and Natural Resources*. March 1, 2018. [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=1C574731-A9C0-4E1C-9E05-15C492E332B1](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1).
- Weiss, Walter. "Rapid Attack Detection, Isolation and Characterization Systems (RADICS)." Defense Advanced Research Projects Agency. n.d. <https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems>.
- Western Electricity Coordinating Council. "Conservative System Operations." Training slides. n.d. <http://docplayer.net/55224883-Conservative-system-operations.html>.
- The White House. *National Security Strategy of the United States of America*. Washington, DC: The White House, December 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- "Work Continues on ITC Lake Erie Project." *Transmission Hub*, February 19, 2018. <https://www.transmissionhub.com/articles/2018/02/work-continues-on-itc-lake-erie-project.html>.



## Acknowledgments

My special thanks go to Robert Denaburg, senior analyst at Sonecon LLC. I also thank the following colleagues for helpful reviews of this study: Michael Assante (SANS Institute); Wayne Austad (Idaho National Laboratory); Terry Boston; Stuart Brindley; Gerry Cauley; Richard Danzig (JHU/APL); Daniel Elmore (Idaho National Laboratory); Peter Grandgeorge (Berkshire Hathaway Energy); Emily Goldman (US Cyber Command); Sean Griffin (ecubed us LLC); Dave Halla (JHU/APL); Jon Jipping (ITC Holdings); Debra Lavoy (Narrative Builders); Bill Lawrence (NERC); Joseph Maurio (JHU/APL); James Miller (JHU/APL); Michael Moskowitz (JHU/APL); Richard Mroz; Steven T. Naumann (Exelon Corporation); Catherine Peacock (JHU/APL); Emilia Probasco (JHU/APL); Erin Richardson (JHU/APL); David Roop (Dominion Energy); Matthew Schaffer (JHU/APL); senior leaders at Southern Company; Kyle Thomas (Dominion Virginia Power); and Virginia Wright (Idaho National Laboratory). I also thank the many additional industry and government reviewers who preferred to remain anonymous.

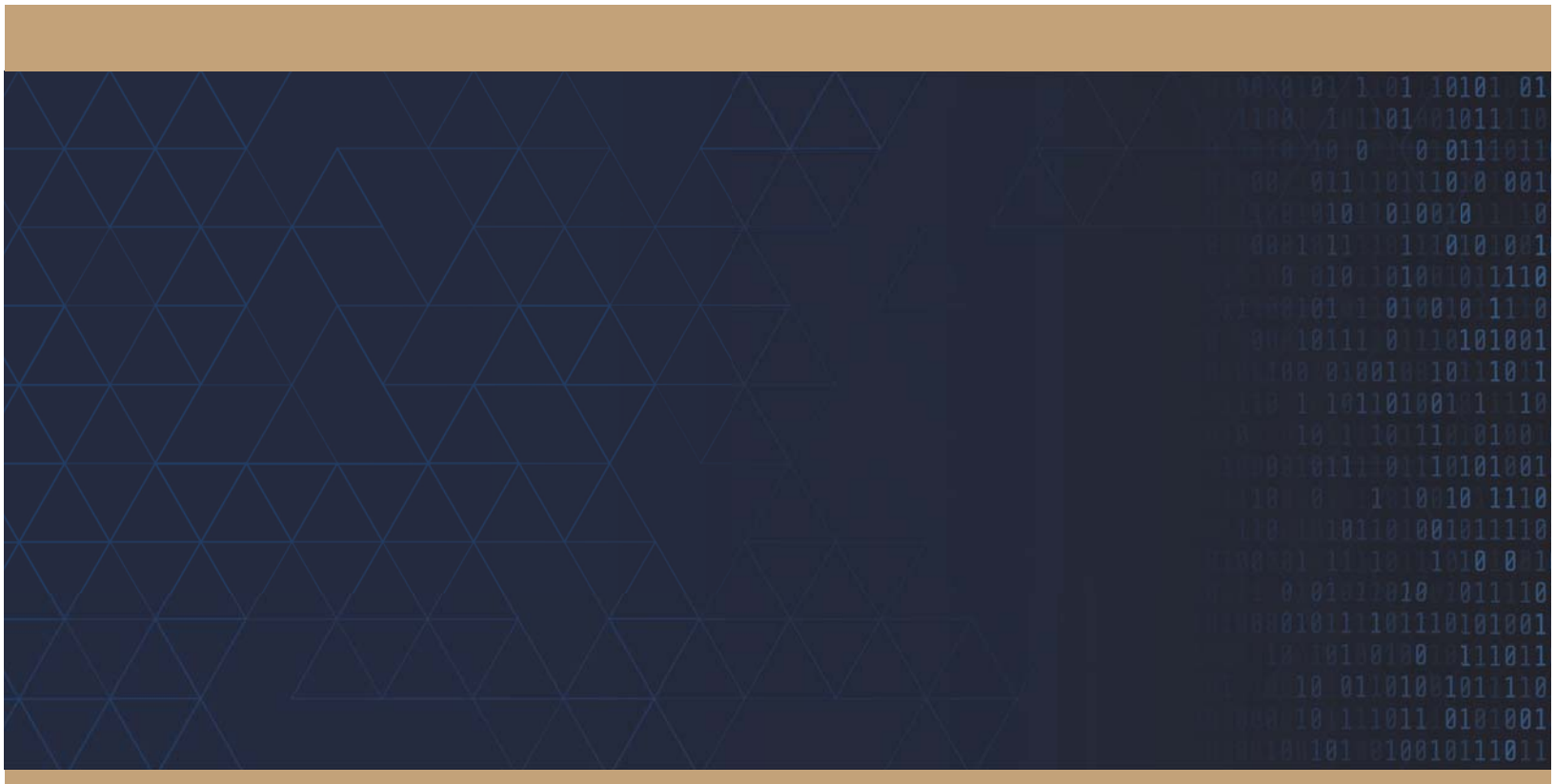
## About the Author

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC, and a senior fellow of JHU/APL. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support in Superstorm Sandy and other disasters. Dr. Stockton also served as the Department of Defense (DOD) domestic crisis manager and was responsible for defense critical infrastructure protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors and was responsible for developing and overseeing the implementation of DOD security policy in the Western Hemisphere. Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation, associate provost of the Naval Postgraduate School, and director of the school's Center for Homeland Defense and Security. Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the author of *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System* (Laurel, MD: JHU/APL, 2016) and numerous other publications. He served as the facilitator of the GridEx IV exercise (November 2017) and is a member of the Homeland Security Advisory Council and other public and private sector boards.









**To:** Joe McClelland

**Through:** (b) (6), David Andrejcak, Harry Tom

**From:** (b) (6)

**Subject:** Summary of “Enhancing the Resilience of the Nation’s Electricity System”

**Date:** March 20, 2018

**I. Introduction**

(b) (5)

[Redacted text block]

(b) (5)

**II. Summary of Study Report**

(b) (5)

[Redacted text block]

[Redacted text block]

[Redacted text block]

---

<sup>1</sup> Available at <http://nap.edu/24836>

(b) (5)





(b) (5)

A large rectangular area of the document is completely redacted with a solid black box. The redaction covers approximately the top third of the page content.A large rectangular area of the document is completely redacted with a solid black box. This redaction covers the middle section of the page, below the first redacted block.A large rectangular area of the document is completely redacted with a solid black box. This redaction covers the bottom section of the page, below the second redacted block.

(103). Recommendation 5.5 is for the DOE and DHS to “evaluate and recommend the  
(b) (5)

[Redacted]

[Redacted]

[Redacted]

(b) (5)

(b) (5) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

(b) (5) [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]



(b) (5) [Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

**From:** [David Andrejcek](#)  
**To:** [Joseph McClelland](#)  
**Subject:** FW: Resilience Report  
**Date:** Friday, March 30, 2018 9:54:04 AM  
**Attachments:** [NAP resilience summary.docx](#)  
[Enhancing the Resilience of the Nations Electricity System.pdf](#)

---

I can't recall when you asked for this but once again, (b) (6) did a nice job!

---

**From:** (b) (6)

**Sent:** Thursday, March 22, 2018 10:36 AM

**To:** Harry Tom <Harry.Tom@ferc.gov>; (b) (6) David Andrejcek  
<David.Andrejcek@ferc.gov>

**Cc:** Andrew Dodge <Andrew.Dodge@ferc.gov>

**Subject:** Resilience Report

Harry, (b) (6), and Dave,

Attached is a requested draft summary of the National Academies report on Resilience. I've added Dave A to this distribution and cc'd Andy for his information.

I've attached a PDF of the report. I have Joe's hard copy – I can return it via Rose.

(b) (6)

Federal Energy Regulatory Commission  
Office of Energy Infrastructure Security

(b) (6)

# RESILIENCE FOR **GRID SECURITY** EMERGENCIES

**Opportunities for Industry–Government Collaboration**

**National Security Perspective**



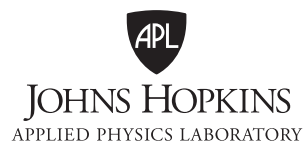
Paul N. Stockton



# **RESILIENCE FOR GRID SECURITY EMERGENCIES**

Opportunities for Industry–Government Collaboration

Paul N. Stockton





Copyright © 2018 The Johns Hopkins University Applied Physics Laboratory LLC. All Rights Reserved.

This National Security Perspective contains the best opinion of the author at time of issue. The views expressed in this study are solely those of the author and do not necessarily reflect the opinions, practices, policies, procedures, or recommendations of the US Department of Energy or any other US government agency or of JHU/APL sponsors.

## Contents

Figures.....	v
Summary .....	vii
<b>Developing Emergency Orders under the FPA.....</b>	<b>1</b>
Drafting Template Emergency Orders before Attacks Occur .....	3
Participants in Drafting and Implementing Emergency Orders .....	5
Goals and Specific Design Requirements for Developing Emergency Orders .....	11
<b>Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies .....</b>	<b>13</b>
Threats That Can Trigger Grid Security Emergencies .....	13
Thresholds for Declaring Grid Security Emergencies .....	17
Data Sharing and Consultations with Industry .....	25
<b>Grid Security Emergency Phases and Order Design Options .....</b>	<b>28</b>
Preattack Options.....	29
Extraordinary Measures when Attacks Are Occurring.....	33
Emergency Orders to Support Power Restoration.....	35
<b>Additional Emergency Order Design Parameters and Supporting Initiatives .....</b>	<b>38</b>
Deterring and Defeating US Adversaries.....	38
Communications Requirements for Issuing and Employing Emergency Orders .....	46
The Deeper Value Proposition for Emergency Orders.....	52
<b>Conclusions and Recommendations for Broader Progress .....</b>	<b>58</b>
Employing Additional Emergency Authorities for Cross-Sector Resilience.....	59
Extended Partnership Requirements within the United States and Abroad.....	64
Playing Defense in Cyberwarfare .....	70
Bibliography .....	75
Acknowledgments.....	93
About the Author .....	93



Figures

Figure S-1. Grid Security Emergency Phases..... viii

Figure 1. Stakeholders for Building Grid Security Emergency Resilience.....10

Figure 2. ODNI Cyber Threat Framework.....20

Figure 3. Elements of the Cyber Incident Severity Schema .....21

Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies.....26

Figure 5. Emergency Order Matrix: Examples of Order Designs .....29

Figure 6. Categories for Protecting Defense Critical Electric Infrastructure .....41

Figure 7. NERC Regional Entities across North America .....67

Figure credits:

Figure 2: “The Cyber Threat Framework,” ODNI (Office of the Director of National Intelligence), n.d., <https://www.dni.gov/index.php/cyber-threat-framework>.

Figure 3: DHS (US Department of Homeland Security), *National Cyber Incident Response Plan* (Washington, DC: DHS, December 2016).

Figure 7: Information from NERC (North American Electric Reliability Corporation), <http://www.nerc.com/Pages/default.aspx>; figure reprinted from Susan Lee, Michael Moskowitz, and Jane Pinelis, *Quantifying Improbability: An Analysis of the Lloyd’s of London Business Blackout Cyber Attack Scenario*, National Security Report NSAD-R-18-027 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018).





## Summary

The US Congress has opened the door to novel strategies for defending the country's electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act (FPA) in December 2015, Congress granted the secretary of energy vast new authorities to use when the president declares a grid security emergency. Most important, the secretary can issue emergency orders to power companies to protect and restore grid reliability when attacks on their systems are "imminent" or under way.<sup>1</sup> The FPA is silent, however, on what the secretary might require companies to do and how such orders can bolster their emergency operations.

The onset of an attack would be the worst possible time to develop emergency orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid. They could then adjust such orders to fit the specific circumstances of an attack. Developing emergency orders in advance would also help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. Companies could then exercise their contingency plans to build preparedness for response operations and contribute to national security in unprecedented ways.

This report is structured to help the electricity subsector and Department of Energy (DOE) develop emergency orders to defend the grid against potentially catastrophic cyber and physical attacks. The report highlights the phases that grid security emergencies are likely to entail. It analyzes the requirements that emergency orders will need to meet for each phase, and how orders can supplement existing utility plans and capabilities to fill gaps in grid resilience. The report also examines how emergency orders can strengthen deterrence against grid attacks and help defeat adversaries if deterrence fails.

The president must declare a grid security emergency before the secretary of energy can issue emergency orders. However, the FPA offers only broad and potentially ambiguous criteria for making that determination, especially for attacks that are imminent. Such ambiguity is useful; the president should retain the flexibility to declare grid security emergencies in a wide range of circumstances. Nevertheless, policy makers may find it useful to establish more detailed criteria to support their internal deliberations. This report proposes options for them to consider, including criteria derived from the electric industry's requirements to preserve "adequate levels of reliability" against cascading blackouts and other multistate grid disruptions. The report also examines how industry and government agencies can refine their information sharing mechanisms to support the emergency declaration process.

Once the president makes such a declaration, grid security emergencies may roll out in three phases, each of which provides the basis for developing a distinct set of template emergency orders. Figure S-1 illustrates these phases. The first will occur if the president determines that an attack is imminent. A well-established basis already exists for developing preattack emergency orders. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions. Such operations might include staffing up emergency operations centers, prepositioning recovery personnel and supplies, increasing available generation to help manage grid instabilities, and taking other precautionary measures. A key advantage of many of these options is that utilities can carry them

---

<sup>1</sup> Fixing America's Surface Transportation Act, Public Law 114-94.

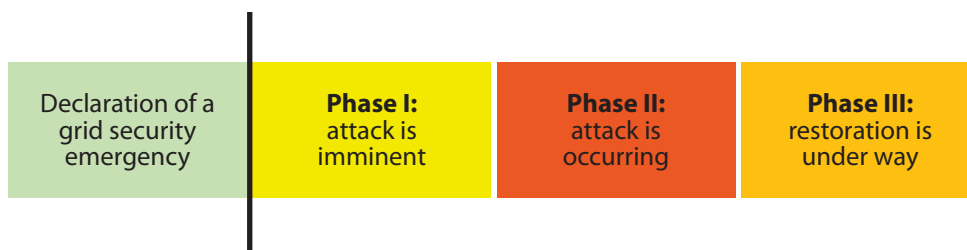


Figure S-1. Grid Security Emergency Phases

out without disrupting normal service; if the hurricane veers back to sea, utilities will have no regrets about having implemented them.

Power companies should help DOE develop equivalent “no-regrets” conservative operations to protect the grid against imminent cyber and physical attacks. A growing number of utilities are already adapting their existing plans for conservative operations to counter physical and cyber risks. These initiatives provide a strong foundation for developing emergency orders that will leverage best practices and help ensure that utilities will implement them on a consistent, nationwide basis. Moreover, because many of these conservative operations will inflict little or no disruption on normal grid service, they are ideal for protecting the grid when attacks are increasingly probable but not certain to occur. DOE and industry should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The next phase of grid security emergencies will occur when attacks are under way. Emergency orders for this phase can help utilities prevent power failures from cascading across the United States and prioritize the sustainment of electric service for military bases and facilities essential for public health (e.g., major regional hospitals and metropolitan water systems). As with conservative operations, existing electric industry plans and capabilities provide a strong basis for developing such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Orders for equivalent *extraordinary measures* could provide useful arrows in the quiver in grid security emergencies.

The final phase of grid security emergencies will commence as utilities begin restoring service to areas without power. Attacks that damage or destroy large numbers of high-voltage transformers and other difficult-to-replace grid components could create outages that darken major portions of the United States for many weeks, or even months. Power companies and DOE already have initiatives under way to meet this challenge. They should also collaborate to develop emergency orders to *support restoration*, which could facilitate the movement of replacement transformers and assist utilities in other strategically vital ways.

These grid security emergency phases could overlap. In particular, once power companies begin restoring power, adversaries may launch follow-on attacks that necessitate continued load shedding and other extraordinary measures to protect grid reliability. At the outset of an emergency, utilities should prepare to receive and implement orders across all emergency phases in an integrated way.

DOE and its industry partners should also design emergency orders to fill underlying gaps in preparedness for cyber and physical attacks. Power companies already have extensive plans and capabilities to protect and restore grid reliability against these threats, in part because mandatory reliability standards require them to do so. Grid owners and operators are also spring-loaded to employ emergency measures the moment they are

needed. Indeed, the North American Reliability Corporation can fine most major US power companies if they fail to implement emergency actions to protect grid reliability.<sup>2</sup> This robust industry preparedness begs the question: what added value can DOE emergency orders provide?

The most obvious benefit lies in the FPA's provisions for regulatory waivers and cost recovery. When grid owners and operators carry out emergency orders, they may have to violate environmental standards and other regulatory requirements. The FPA now protects entities from being punished for such violations if they occur while complying with emergency orders. The act also provides for the recovery of costs that companies will incur in implementing emergency orders. This report examines how further waiver and cost-recovery measures could reinforce preparedness for grid security emergencies.

Emergency orders can also help support national security in new and far-reaching ways. Russia, China, and other potential adversaries will not strike the grid simply to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to US defense installations responsible for deploying forces to the region, as well as to ports and other civilian infrastructure that supports force projection. Emergency orders can be designed to help deter—and, if necessary, defeat—such attacks. This report proposes specific options to do so, in support of the *National Security Strategy of the United States of America* and other sources of US policy guidance.

Some of these options will require harsh and politically contentious decisions on allocating power if adversaries severely disrupt the grid. Emergency orders for prioritized load shedding provide a case in point. To help deter attacks, grid owners and operators need the ability to sustain service to critical defense installations, including those responsible for conducting response operations against (and imposing costs on) potential attackers for however long a conflict may last. The ability to protect power flows to hospitals and other facilities vital for public health and safety will be valuable as well. However, if adversaries disrupt sufficient grid generation and transmission assets, sustaining reliable service to these installations may require utilities to curtail service to other customers. Government officials—and, ultimately, the president—should make such decisions and provide political top cover and liability protections for power companies that implement them.

Grid security emergencies will also create unprecedented challenges for government and industry to communicate with the American people. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Against a backdrop of fear and uncertainty, adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks. Adversaries may also disrupt the phone and internet-based communications systems utilities typically use to coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications playbooks to prepare for grid security emergencies, and they should make doing so a core component of the emergency order development process.

DOE and its industry and government partners will need to conduct intensive follow-on work to finalize the development of emergency orders and build utility-specific contingency plans to implement the orders in ways that account for accelerating structural changes in the electricity subsector. Their collaborative efforts will

---

<sup>2</sup> Bulk power system entities, including generation and high-voltage transmission companies, are subject to NERC's mandatory reliability standards and emergency orders under the FPA. For an analysis of applicability issues, see pages 5–10.

require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, as utilities and DOE tackle the immediate challenges of developing emergency orders, they should also explore broader opportunities to build preparedness for grid security emergencies. One such opportunity lies in integrating the use of emergency orders with other federal authorities. The secretary of energy can issue grid security emergency orders only to power companies. Increasingly, however, power generation depends on the flow of natural gas. Communications systems and other infrastructure sectors will also play critical roles in supporting power restoration. The secretary of energy and other federal leaders have additional authorities beyond section 215A of the FPA that can strengthen cross-sector resilience for grid security emergencies. However, achieving these benefits will require private and public sector leaders to preplan and exercise the coordinated use of these authorities, and to develop “whole-of-government” strategies to support infrastructure owners and operators.

Coordination with Canada could be valuable as well. The electric grids of the United States and Canada are deeply interconnected, and adversary-induced failures in one nation may rapidly cascade into the other. The secretary of energy does not have the authority to issue emergency orders to power companies in Canada (or in any other nation). Yet, significant opportunities exist to build on current reliability protections and emergency coordination mechanisms between US and Canadian utilities. The United States could also develop collaborative plans with Mexico as well as US allies in Europe and Asia.

In addition, DOE and its partners should explore further opportunities to help deter cyber attacks and defeat US adversaries if deterrence fails. The US *National Security Strategy* emphasizes that the United States needs to convince adversaries not only that they will suffer costly consequences if they attack but also that attacking will not accomplish the objectives they seek—in other words, achieve deterrence by denial. Yet, leading scholars of deterrence argue that deterrence by denial will be extraordinarily difficult to establish in cyberspace. Emergency orders and implementation plans can help meet these challenges by strengthening grid resilience in novel ways. Government agencies should also consider developing broader doctrine to “play defense” if cyberwarfare breaks out, and coordinate grid security emergency operations at home with measures to suppress adversary attacks at their source.

The foundational importance of the electric grid makes it a prime target for attack. As secretary of energy Richard Perry emphasizes, “America’s greatness depends on a reliable, resilient electric grid” that can power the economy, support national defense, and provide for the necessities of modern life.<sup>1</sup> To prevent adversaries from exploiting the United States’ dependence on the grid, the Department of Energy (DOE) and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter—and, if necessary, defeat—attacks on the grid.<sup>2</sup>

The FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the Fixing America’s Surface Transportation (FAST) Act amendments to the FPA, it greatly expanded the secretary of energy’s authority to issue emergency orders to grid owners and operators. Under section 215A of the act, “the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability” of critical electric infrastructure in a grid security emergency.<sup>3</sup> Before the secretary can issue those orders, the president

must first declare a grid security emergency when attacks on the grid are imminent or under way.<sup>4</sup>

However, legislators provided scant guidance on what the secretary might order power companies to do. DOE and its partners in the electricity subsector are now assessing which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats. This report supports their work by examining possible emergency orders and analyzing broader opportunities to strengthen resilience for grid security emergencies.

## Developing Emergency Orders under the FPA: Collaborative Opportunities, Fundamental Goals, and Overarching Design Requirements

The secretary of energy’s new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, “the nine most terrifying words in the English language are ‘I’m from the government and I’m here to help.’”<sup>5</sup> Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already taking steps to minimize such risks. Especially valuable, the department has incorporated industry recommendations on the process by which the secretary should issue emergency orders to utilities, and—“if practicable”—consult with industry before those orders are issued.<sup>6</sup> The next collaborative step should be to include power companies in

<sup>1</sup> Perry, letter to the FERC.

<sup>2</sup> The 2015 FAST Act amendments to the FPA provide the authority to undertake these efforts. Prior to 2015, section 202(c) of the FPA already authorized the secretary of energy to issue emergency orders to order “temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest.” That provision also specified that the secretary could exercise such powers “during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes.” See “DOE’s Use of Federal Power Act Emergency Authority,” DOE. The 2015 FAST Act amendments to the FPA gave the secretary further powers (mostly incorporated in section 215A of the act), which are the primary focus of this report.

<sup>3</sup> 16 U.S.C. § 824o, (b)(1).

<sup>4</sup> The analysis that follows examines the definition of such emergencies in the FPA and potential thresholds for declaring them.

<sup>5</sup> Reagan, “President’s News Conference.”

<sup>6</sup> DOE, “RIN 1901–AB40,” 1176; EEI, “Comments”; and Paradise et al., “ISO-RTO Council Comments.”



designing template emergency orders. Grid owners and operators have unequaled knowledge of their own infrastructure and operating procedures and extensive experience in employing emergency measures to protect and restore grid reliability.<sup>7</sup> They are well positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses—and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders would be most useful to help defend their systems and effectively supplement the emergency measures utilities would already be taking on their own. Utilities will also play a critical role in building company-specific plans to implement emergency orders, exercising those plans, and identifying remaining gaps to fill.

Strategic guidance from DOE and other government departments will be just as critical for designing emergency orders. Federal leadership will be essential to ensure that emergency orders help achieve overarching US security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing emergency orders to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.<sup>8</sup> Government officials can also shape emergency orders and supporting initiatives to help implement US cyber resilience strategies, including the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

(May 2017) and DOE's *Multiyear Plan for Energy Sector Cybersecurity* (March 2018).<sup>9</sup>

In addition, DOE will play a critical role in coordinating industry and government operations during grid security emergencies. The same congressional amendments that granted the secretary expansive new emergency authorities also specified that DOE shall be the federal government's "lead sector-specific agency for cybersecurity for the energy sector." As such, the secretary is responsible for collaborating with grid owners and operators, regulators, and other government agencies to help mitigate incidents and provide broader support to the energy sector.<sup>10</sup>

Federal incident response operational plans provide a broader framework for building these collaborative mechanisms. Presidential Policy Directive 41, *United States Cyber Incident Coordination* (July 2016), the *National Cyber Incident Response Plan* (December 2016), and the *National Response Framework* (June 2016) offer particularly useful guidance for building grid-specific coordination mechanisms.<sup>11</sup> DOE is also strengthening its own internal mechanisms and organizational structure to manage cyber incidents.<sup>12</sup> These changes further position the department to effectively collaborate with industry in developing and executing emergency orders.

<sup>9</sup> Trump, *Executive Order on Strengthening Cybersecurity*; and DOE, *Multiyear Plan*. See also Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*; and DHS, *Cybersecurity Strategy*.

<sup>10</sup> Fixing America's Surface Transportation Act, Public Law 114-94, 1779 (hereafter cited as FAST Act).

<sup>11</sup> Obama, *United States Cyber Incident Coordination*; DHS, *National Cyber Incident Response Plan*; and DHS, *National Response Framework*.

<sup>12</sup> DOE, *Multiyear Plan*, 28. DOE has also established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to "enable more coordinated preparedness and response to natural and man-made threats." See "Secretary of Energy Forms New Office," DOE.

<sup>7</sup> FERC and NERC, *Restoration and Recovery Plans*; FERC and NERC, *Planning Restoration Absent SCADA or EMS (PRASE)*; and FERC and NERC, *Recommended Study: Blackstart Resources Availability (BRAv)*. Additional BPS plans, exercises, and mandatory reliability standards are addressed in subsequent portions of the report.

<sup>8</sup> White House, *National Security Strategy*.

## Drafting Template Emergency Orders before Attacks Occur

The FPA specifies that before issuing emergency orders “the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action,” consult with appropriate power companies and other grid resilience stakeholders.<sup>13</sup> But opportunities for such consultations may be sharply limited. Adversaries may strike the grid with little or no warning. Moreover, when attacks are imminent or under way, rapidly issuing emergency orders may be crucial to help prevent cascading failures and other widespread disruptions. This imperative for speed could make consultations impractical.

To enable collaboration and minimize the risk that DOE will have to create orders amid the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, assistant secretary of energy for electricity delivery and energy reliability, stated in March 2018: “In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.”<sup>14</sup> Power companies and other electricity subsector organizations have also emphasized the need for industry and the government to jointly develop orders before adversaries strike.<sup>15</sup>

Such collaborative efforts should initially focus on creating *template orders*: orders that lay out the

basic types of actions that the secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act amendments’ potential value for the secretary to issue general orders to “protect and restore the reliability of the grid.” Vague, overly broad directives cannot provide an adequate basis for utilities to develop system-specific plans to implement them. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for “maximum generation” and increased reserve margins to more aggressive, far-reaching measures.<sup>16</sup> A key objective for such development efforts: provide a menu of agreed-upon options from which the secretary can choose as circumstances require, supported as much as possible by consultations with industry.

Developing emergency orders before attacks occur can help ensure that, as a minimalist goal, such orders will “do no harm.” By participating in the order design process, power companies can shape orders to account for system-specific engineering constraints and requirements for emergency operations. This industry input will be especially important because DOE has the authority to punish utilities for failing to comply with emergency orders, even if they are poorly designed. DOE’s grid security emergency rule specifies that “in accordance with available enforcement authorities, the secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order.”<sup>17</sup> If

<sup>13</sup> This includes the North American Electric Reliability Corporation (NERC) and its Electricity Information Sharing and Analysis Center (E-ISAC). 16 U.S.C. § 824o–1. See also the notice of proposed rulemaking and request for comment (DOE, “RIN 1901–AB40”).

<sup>14</sup> Walker, *Written Testimony*.

<sup>15</sup> See Joint Commenters, “Comments; and NASEO, “Comments.”

<sup>16</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual* 13, 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help “maintain reliable operation while meeting . . . unexpected outages of existing capacity.” See “M-1 Reserve Margin,” NERC.

<sup>17</sup> DOE, “RIN 1901–AB40,” 1182.

power companies find that an order is impossible to implement or is otherwise objectionable, they can ask DOE to reconsider it.<sup>18</sup> But adjudicating individual emergency orders amid a grid security emergency could delay time-critical actions. Instead, DOE should include industry in developing emergency orders from the start and resolve utility concerns before adversaries strike.

Preplanning to coordinate industry and government emergency operations will also be valuable. Power companies are already poised to take immediate emergency actions to protect grid reliability as circumstances require, regardless of whether the secretary issues emergency orders. It will be helpful to understand in advance how DOE can best align the issuance of such orders with industry-initiated actions. Once attacks are under way, preplanning for operational coordination will become still more important, especially if adversaries continue striking the grid and its supporting communications systems after their initial salvo.

If attacks do occur, Russia, China, or other potential adversaries will use country-specific tactics, techniques, and procedures to disrupt US infrastructure. Defending against those attacks will require tactical and operational responses that are similarly tailored to specific adversaries. Over time, it may be possible to develop (and protect adversaries from accessing) emergency orders that account for these individualized defensive requirements. US leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this report examines opportunities to do so.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders

should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high-voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military bases, regional hospitals, and other critical customers that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and identify opportunities to improve order design and execution. Training programs to prepare employees to carry out utility-specific implementation plans should also get under way as soon as possible. On a larger scale, utilities will also be able to exercise the implementation of template emergency orders within the framework of the Cyber Mutual Assistance (CMA) Program. This program enables over 140 utilities in the United States and Canada to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.<sup>19</sup> Exercises can help determine how best to align the issuance and implementation of emergency orders with these growing capabilities for mutual support.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the secretary of energy has the sole authority to issue emergency orders, the secretary may request input from senior DOE staffers

<sup>18</sup> DOE, "RIN 1901-AB40," 1181-1182.

<sup>19</sup> "ESCC's Cyber Mutual Assistance Program," ESCC.

on which orders will be most useful against specific types of attacks. The secretary may also need to brief the president and the National Security Council on proposed orders and their potential benefits. By developing orders and clarifying their respective advantages before adversaries strike, DOE and industry partners can facilitate such deliberations.

Over the longer term, industry and government leaders might structure their collaboration to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public-private and interagency coordination.<sup>20</sup> Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government-industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, to develop template emergency orders and contingency plans to implement them, power companies will need to conduct extensive operational and engineering studies and use enhanced modeling to understand the potential impact of such orders. The FAST Act amendments to the FPA provide no funding for such development efforts. Moreover, DOE and power companies are only the most obvious participants in the order design process. A wide array of other grid resilience and incident management stakeholders may also need to assist that process—including critical ones not mentioned in the FPA. Determining which specific public and private sector organizations should help shape template orders constitutes a critical first step in preparing for grid security emergencies.

## Participants in Drafting and Implementing Emergency Orders: The Bulk Power System and the Broader Electricity Subsector

An initial task in developing emergency orders will be to determine which components of the electricity subsector should participate in that effort. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>21</sup> The most obvious candidates for inclusion are the power companies that are subject to emergency orders. The FAST Act amendments to the FPA specify which components fall into that category. Chief among them are “any owner, use or operator of critical electric infrastructure or of defense critical electric infrastructure within the United States.”<sup>22</sup> The FPA also includes criteria to identify this infrastructure. Critical electric infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>23</sup> Defense critical electric infrastructure consists of grid components that serve facilities “critical to the defense of the United States” and that are vulnerable to the disruption of grid-provided power.<sup>24</sup>

However, Congress also narrowed the definition of critical electric infrastructure in a significant way. The FPA states that such infrastructure only includes assets that compose the bulk power system (BPS). BPS assets are those “facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation

<sup>20</sup> Danzig, *Catastrophic Bioterrorism*, 5–7; and Blue Ribbon Study Panel, *National Blueprint*, 13, 42–44.

<sup>21</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>22</sup> 16 U.S.C. § 824o–1, (b)(4)(c).

<sup>23</sup> 16 U.S.C. § 824o–1, (a)(2).

<sup>24</sup> 16 U.S.C. § 824o–1, (a)(4).



facilities needed to maintain transmission system reliability.”<sup>25</sup> These BPS generation and transmission assets provide synchronized power within the three interconnections that serve the entire United States and parts of Mexico and Canada.<sup>26</sup>

As defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.<sup>27</sup> That limitation creates a potential problem for executing emergency orders. Local distribution systems often provide the “last mile” of connectivity between transmission systems and military bases and other critical customers. As DOE and industry create template emergency orders and execution plans, it will be essential to integrate local distribution providers into that development process.

However, before examining these distribution-level issues, it will first be helpful to clarify the components of the BPS that are explicitly subject to emergency orders under the FPA (and are therefore key partners for DOE in designing them). The FPA states that the secretary of energy may issue emergency orders to the following the BPS “entities:”<sup>28</sup>

**The Electric Reliability Organization.** After blackouts cascaded across major portions of the United States in August 2003, Congress authorized the Federal Energy Regulatory Commission (FERC) to certify an electric reliability organization to develop and enforce, subject to FERC approval, mandatory

electric reliability standards for all users, owners, and operators of the US BPS.<sup>29</sup> FERC certified the North American Electric Reliability Council (NERC) as the first-ever electric reliability organization in July 2006. Renamed the North American Electric Reliability Corporation in 2007, it has served in that role since.<sup>30</sup> NERC’s mission is to ensure the reliability and security of the BPS in North America. As such, NERC is uniquely positioned to help DOE develop emergency orders, especially for attacks that could create cascading blackouts or other multistate disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a leading role for the electricity subsector in establishing situational awareness, incident management and coordination, and communication capabilities.<sup>31</sup> E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be vital for responding to grid security emergencies.

**Regional entities responsible for enforcing reliability standards for the BPS.**<sup>32</sup> NERC has delegated certain authorities to eight regional entities to monitor and enforce compliance with reliability standards.<sup>33</sup> While regional entities play major oversight roles, they do not directly operate the physical grid and would not, on their own, be positioned to execute emergency orders. However, they could help utilities and DOE and preplan for

<sup>25</sup> 16 U.S.C. § 824o, (a)(1).

<sup>26</sup> Interconnections are defined as the “geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control.” North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See NERC, *Glossary*.

<sup>27</sup> The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify “local” distribution. See 16 U.S.C. § 824o, (a).

<sup>28</sup> 16 U.S.C. § 824o–1, (b)(4).

<sup>29</sup> Energy Policy Act of 2005, Public Law 109-58. This does not include Alaska or Hawaii.

<sup>30</sup> NERC, *History*. For more information on NERC, see “About NERC,” NERC.

<sup>31</sup> “Electricity Information Sharing and Analysis Center,” NERC.

<sup>32</sup> DOE, “RIN 1901–AB40,” 1177. See also 16 U.S.C. § 824o, (a)(7).

<sup>33</sup> “Key Players,” NERC. In July 2017, however, one regional entity announced its intention to dissolve. FERC has approved the dissolution, effective July 2018. See FERC, *Order Granting Approvals* (163 FERC ¶ 61,094).



issuing regulatory waivers to BPS grid operators as they comply with emergency orders.

**Owners, users, and operators of critical electric infrastructure or defense critical electric infrastructure within the United States.**<sup>34</sup> Companies that own and operate generation and transmission assets will be among the most likely recipients of emergency orders and should play a critical role in designing them. Reliability coordinators will be similarly important. Reliability coordinators are the entities that constitute “the highest level of authority” for the reliable operation of the bulk electric system (BES).<sup>35</sup> They are also responsible for maintaining a “wide-area view” of the BES and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, reliability coordinators will be critical for designing, receiving, and implementing emergency orders to counter attacks that individual BPS owners and operators may not have the ability to defeat. Seven regional transmission organizations and independent system operators, most of which are registered as reliability coordinators, also help operate and ensure the reliability of the BES in many regions of the United States.<sup>36</sup> Accordingly, regional

transmission organizations and independent system operators will be essential to the design and execution of emergency orders.

### **Local Distribution Providers and Other Grid Resilience Stakeholders**

The 2015 FAST Act amendments to the FPA do not explicitly address the possible roles of local distribution systems in grid security emergencies. However, local distribution infrastructure is critical for overall resilience against cyber and physical attacks. Even if emergency orders help defeat attacks on BPS assets, adversaries may still be able to achieve catastrophic effects by striking multiple local distribution systems and thereby interrupting the flow of power from transmission systems to military bases, hospitals, and other end users. Local distribution systems may also need to help implement emergency orders issued to BPS entities. For example, if the secretary orders transmission systems to protect reliability by shedding load, yet at the same time sustain the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding. Holistic preparedness for grid security emergencies therefore requires engagement with local distribution systems.

These systems will also have strong incentives to participate in the emergency order planning process. Just as BPS entities rely on local distribution utilities, these utilities rely on generation, transmission, and higher-voltage distribution entities to serve end users. Local systems will also share the commitment of BPS entities to protect and rapidly restore service to defense installations and other critical customers. By integrating local distribution utilities

<sup>34</sup> The analysis that follows later in this section examines the definition of “users” of critical electric infrastructure and defense critical electric infrastructure.

<sup>35</sup> While the BPS broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the BES is a subset of the BPS that includes, with some exclusions, all transmission and real and reactive power sources at one hundred kilovolts or higher. As with the BPS definition, the BES definition excludes local distribution providers. For these definitions, as well as the definition of reliability coordinators, see NERC, *Glossary*. Consistent with the FPA and the authorities it provides for handling grid security emergencies, this report focuses on the application of emergency orders to BPS entities specifically.

<sup>36</sup> There are ten regional transmission organizations and independent system operators under NERC’s purview, though three operate exclusively in Canada. Regional transmission organizations and independent system operators are independent membership-based nonprofit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are

operated by individual utilities or utility holding companies. See “About 60% of U.S. Electric Power Supply Managed by RTOs,” US Energy Information Administration. Six of the seven regional transmission organizations/independent system operators operating in the US are also current reliability coordinators. See “Reliability Coordinators,” NERC.

into emergency order planning, these utilities will be able to participate in shaping template orders and implementation plans to help achieve their reliability goals when adversaries strike. Moreover, to the extent that local distribution companies may be subject to emergency orders, they may also benefit from the FPA's liability protections and cost-recovery provisions for actions taken to execute those orders.

DOE and other stakeholders may determine that the FPA already gives the secretary adequate authority to issue emergency orders to local distribution companies. The act states that emergency orders may apply to "any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure" within the United States.<sup>37</sup> The act, however, does not further define owners, users, and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the act.

Regardless of whether the secretary can issue orders to local distribution utilities, BPS entities should include them in building the contingency plans to implement emergency orders. This preplanning will be essential to strengthen comprehensive, end-to-end protection of grid reliability against attacks.

Many companies that own transmission assets also own distribution infrastructure. These utilities will find it relatively easy to include distribution assets in their emergency planning. Integrated response plans will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for "vertically integrated" utilities that own and operate assets for all three functions. However, many municipally owned electric utilities and rural electric cooperatives (including those that serve critical and defense critical electric infrastructure) are not part of vertically integrated companies. In US regions where generation, transmission,

and distribution systems exist as separate entities, additional engagement initiatives will be essential to implement emergency orders and sustain power to essential facilities.

Including state regulators and other state officials in these integrative efforts could offer additional benefits. State public utility commissions have primary regulatory jurisdiction over distribution systems.<sup>38</sup> The National Association of Regulatory Utility Commissioners, which represents state regulators nationwide, has focused growing attention on the need for prudent utility investments in cyber and physical resilience.<sup>39</sup> Commissioners in New Jersey and other states are also leading regulatory initiatives to bolster cyber resilience in their respective jurisdictions.<sup>40</sup> Emergency managers and National Guard leaders in a growing number of states are also building new mechanisms to coordinate with utilities in responding to cyber attacks. Adding such additional partners to help design emergency orders and plan for their implementation would complicate an already far-reaching engagement process. Nevertheless, incorporating perspectives from state commissioners and other officials would help advance comprehensive state-level preparedness for grid security emergencies.

### Additional Partners for Engagement

DOE and power companies will need to collaborate with a wider array of partners to develop and execute some potentially useful emergency orders, especially to support grid restoration. The final rule

<sup>37</sup> 16 U.S.C. § 824o, (b)(4)(a).

<sup>38</sup> The US Constitution, in most cases, allows federal regulation of private economic activity only for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See Lazar, *Electricity Regulation in the US*, 15.

<sup>39</sup> See NARUC, *Cybersecurity*; and NARUC, *Resolution on Physical Security*.

<sup>40</sup> State of New Jersey Board of Public Utilities, *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196).

on *Grid Security Emergency Orders: Procedures for Issuance* (hereinafter referred to as the grid security emergency rule) notes: “Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits” to expedite the restoration of power.<sup>41</sup> This includes traditional partners such as the Department of Homeland Security (DHS) and the Department of Defense (DOD). Still broader collaboration with government and private sector partners may be valuable for implementing emergency orders to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy large power transformers at substations across the United States, and these attacks cut off power to critical military bases, the secretary might order industry to prioritize the replacement of large power transformers at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program to provide for such replacements.<sup>42</sup> New industry-led organizations such as Grid Assurance,<sup>43</sup> as well as programs such as the Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) initiative, are further expanding the industry’s capacity to replace transformers and other equipment.<sup>44</sup> These efforts will be essential for preparing for grid security emergencies, especially as industry stocks and securely stores the full range of replacement transformer types and sizes that large-scale physical attacks may require.

However, power companies do not move large power transformers by themselves. They rely on railroad companies, barges, and heavy-haul trucking companies to help do so and have established a

Transformer Transportation Working Group under the ESCC to plan and coordinate transformer movement.<sup>45</sup> Exercises in the Spare Transformer Equipment Program now involve representation from transportation stakeholders. Yet, the FPA does not give the secretary authority to issue orders to transportation companies. In anticipation of orders for replacing transformers, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Preplanning with the US Department of Transportation (DOT), the Federal Emergency Management Agency (FEMA), and state governments to get contracts, permits, and regulatory waivers to expedite transformer movement will also be useful. In addition, advance coordination with emergency managers at all levels of government would help them mitigate the effects of rotating blackouts or other extraordinary measures on public health and safety.

DOE and the electricity subsector should consider expanding the geographic scope of these discussions as well. In defining the defense critical electric infrastructure that emergency orders can protect, Congress excluded grid assets in Alaska and Hawaii.<sup>46</sup> But both states are home to vital military installations, as are a number of US territories. The secretary also lacks the authority to issue emergency orders to Canadian utilities. Yet, US and Canadian electric systems are deeply integrated, and coordinated efforts to prevent instabilities in grid security emergencies could benefit both nations. Collaborations with NATO allies and other security partners in the face of major adversarial cyber campaigns could be valuable as well. The concluding section of this report examines the potential benefits of expanding grid

<sup>41</sup> DOE, “RIN 1901–AB40,” 1177.

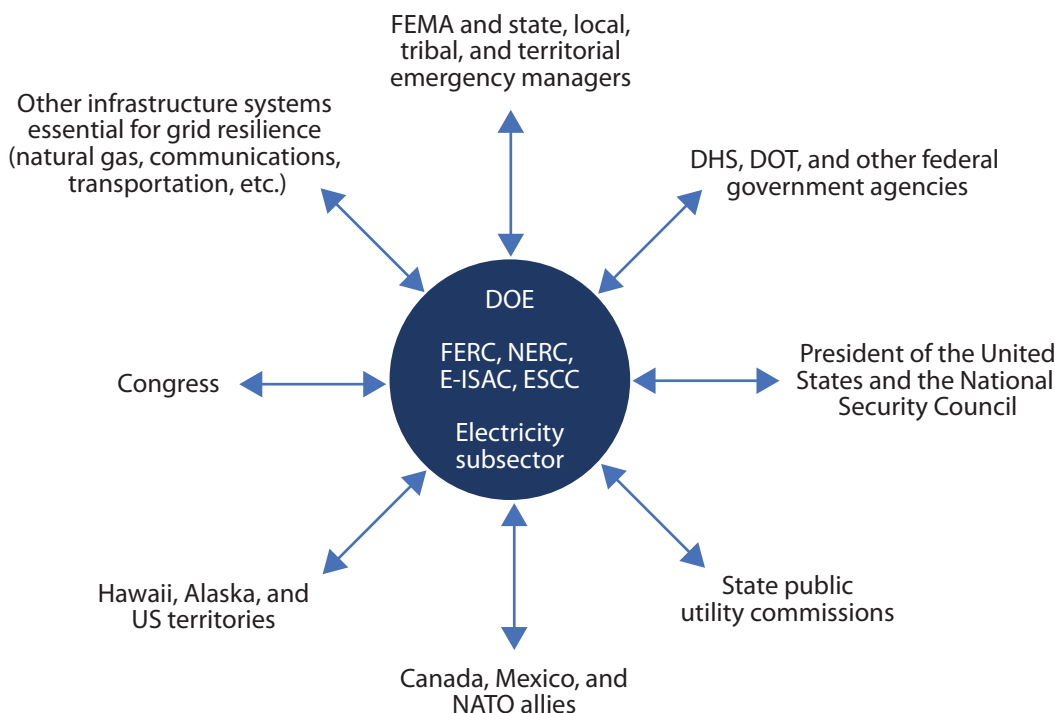
<sup>42</sup> See DOE, *Strategic Transformer Reserve*; and “Spare Transformers,” EEL.

<sup>43</sup> “Transmission Equipment Ready,” Grid Assurance.

<sup>44</sup> FERC, *Order Authorizing Acquisition and Disposition* (163 FERC ¶ 61,005), 10.

<sup>45</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>46</sup> 16 U.S.C. § 824o–1, (a)(4). The FPA’s section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).



**Figure 1. Stakeholders for Building Grid Security Emergency Resilience**

security emergency coordination within the United States and beyond.

Figure 1 illustrates the array of partners that might help build preparedness for such emergencies. DOE, BPS entities, and the broader electricity subsector comprise the core of the team needed to design, issue, and implement emergency orders. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>47</sup> This definition comprises the key subsector components represented in the ESCC, to include owners and operators of electric generation, transmission, and distribution assets “from all ownership categories.”<sup>48</sup> As such, the ESCC is ideally suited to coordinate with

DOE in the order development process, together with NERC, the E-ISAC, and other BPS entities and trade associations.

Surrounding these core participants are additional partners that might offer valuable insights for developing orders and coordinating emergency response operations. Some of these partners (including Congress) can also help oversee the implementation of the FPA’s emergency provisions and assess requirements for further statutory changes.

Of course, the full set of potential contributors to emergency preparedness is broader still. For example, vendors who can help utilities replace damaged relays and other equipment could play vital roles. So could law enforcement agencies, cybersecurity contractors, state National Guard organizations, and other sources of expertise and support for power companies. National laboratories and other research and development organizations will also need to sustain their support for improved grid resilience. Over time, comprehensive engagement with all such partners could pay major dividends.

<sup>47</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>48</sup> In addition to infrastructure owners and operators, ESCC membership includes regional transmission organizations and independent system operators, NERC, the National Infrastructure Advisory Council, and the Canadian Electricity Association. ESCC, *Electricity Sub-Sector Coordinating Council Charter*, 3.



## Goals and Specific Design Requirements for Developing Emergency Orders

The starting point in developing template emergency orders is to identify the objectives, scope, and design requirements that these orders will need to encompass. Key issues analyzed in the sections of the report that follow:

- **Threats, triggers, and thresholds for issuing emergency orders.** Only a limited number of natural and man-made hazards can trigger a grid security emergency.<sup>49</sup> Countering each of those hazards will require threat-specific emergency orders. Hence, the first step for developing such orders will be to examine the threats and attack scenarios on which the design process should focus and clarify the criteria that the president might use to determine that a grid security emergency exists—including when there is an “imminent danger” of an attack.
- **Designing emergency orders for sequential phases of grid security emergencies.** Different types of emergency orders will be needed to protect grid reliability (1) when attacks are imminent, and (2) when attacks are under way. Promising opportunities also exist to develop orders for a third phase of grid security emergency operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.
- **Incorporating national security policies and priorities into emergency order design.** Adversaries may strike the grid to disrupt the flow of power to defense installations and other facilities essential to national security. Many utilities are already collaborating with defense partners to build redundant power feeds for these facilities and make other targeted

investments in resilience. A growing number of grid owners and operators also plan to prioritize the restoration of power to military bases if blackouts occur. Emergency orders provide a unique opportunity for DOE and its partners to build on such initiatives, and provide more systematic, comprehensive, and effective support to national security.

An initial step to do so is to ensure that emergency orders reflect and help achieve broader federal government strategies to defend critical infrastructure. Most important, the US *National Security Strategy* specifies how the United States will deter attacks on critical systems and—if deterrence fails—how it will defeat the attackers.<sup>50</sup> DOE and its industry partners should design emergency orders to help implement the strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this design process with two further steps. First, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. The FPA provisions and existing industry plans to prioritize the restoration of power will provide a useful starting point. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement emergency orders and help defend the nation.

Emergency orders and implementation plans also offer a basis to clarify how US agencies and private companies will coordinate their operations during cyberwarfare, and build consensus on the private sector’s emerging role in national security. No power company has ever tried to maximize shareholder value by promising to bolster cyber deterrence or help defeat attacks by nations such as Russia or China. Yet, because

<sup>49</sup> In addition to being triggered by cyber attacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, (a)(7).

<sup>50</sup> White House, *National Security Strategy*, 13.



of the grid's importance to the economy, public health and safety, and national defense, the United States needs a doctrinal framework to coordinate industry and government actions during attacks on the US electric system.<sup>51</sup> Scott Aaronson, Edison Electric Institute's vice president for security and preparedness, notes that "there is not a lot of doctrine around cyber attacks on civilian infrastructure."<sup>52</sup> Building such doctrine and operationalizing public-private partnerships will be crucial for grid security emergency preparedness.

- **Communications.** The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The grid security emergency rule describes the consultative process that (if practicable) will occur before the secretary issues emergency orders.<sup>53</sup> However, the grid security emergency rule does not address the risk that adversaries will attack the industry-government communications systems necessary to issue orders, monitor their implementation, and defeat adversaries' attacks.

Building secure, survivable communications will be essential to effectively issuing and implementing emergency orders. However, the FPA provides no requirements or funding to do so. The electricity subsector is currently working with government agencies and telecommunications companies to advance secure communications initiatives. These partners should treat preparedness for grid security emergencies as a special area of focus, including measures to

ensure that grid owners and operators can verify the authenticity of emergency orders.

Government and utility leaders will also need to coordinate what they tell the American people when the secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including those for prioritized load shedding, could cut off electricity to many thousands of customers. Emergency orders that will have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Attackers will strike the grid to achieve political benefits, including, potentially, the incitement of public panic and a loss of confidence in US leaders. To promote unity of messaging against such efforts, it will be essential to build on existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders.

- **Waivers and cost recovery.** Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the act itself, FERC-approved reliability standards, or environmental regulations.<sup>54</sup> However, emergency orders will be easier to implement if they include preplanned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

<sup>51</sup> For DOD's definition of doctrine and an analysis of its benefits for joint warfighting, see Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United State*.

<sup>52</sup> Lynch, "How the Russian Government Allegedly Attacks."

<sup>53</sup> DOE, "RIN 1901-AB40," 1181.

<sup>54</sup> These waivers apply unless companies carry out orders and related actions in a "grossly negligent manner." See 16 U.S.C. § 824o-1, (f)(4).

The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.<sup>55</sup> Industry–government dialogue will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader preplanning needed for the financial turbulence that grid security emergencies could create. This study also examines possible emergency orders that would require investments in grid infrastructure to implement. The FPA does not authorize government spending on such pre-emergency projects. If DOE and its partners decide that investment-dependent orders have sufficient value for grid resilience, these partners (and Congress) should explore government funding options that reflect the national security benefits of such orders, rather than increase the electricity bills paid by private citizens.

- **Opportunities for broader resilience against grid security emergencies.** Power companies and DOE may find it helpful to develop a comprehensive plan to sequence and integrate all of the initiatives outlined above. Such a plan might also account for three additional opportunities for progress: (1) employing additional government authorities to coordinate emergency operations between electric utilities and companies in other infrastructure sectors, including the natural gas providers on which power generation increasingly depends; (2) deepening US partnerships with Canada to help protect the interconnected North American power grid, and exploring opportunities for collaboration with Mexico and other nations; and (3) examining longer-term opportunities to leverage improvements in grid resilience to strengthen cyber deterrence, and assessing the risks and potential benefits of coordinating cyber defense operations at home and abroad.

## Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies

The FPA leaves the president substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should build consensus on the types of threats that ought to drive and sequence the development process. These partners should also examine possible decision criteria and consultative mechanisms to support declarations of grid security emergencies.

### Threats That Can Trigger Grid Security Emergencies: Implications for Emergency Order Design

A broad array of natural and man-made hazards, including earthquakes and severe weather events such as hurricanes and ice storms, can cause multistate blackouts. However, in amending the FPA, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the “occurrence or imminent danger” of:

(A)

(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;<sup>56</sup> and

(ii) disruption of the operation of such devices or networks, with significant adverse

<sup>55</sup> 16 U.S.C. § 824o–1, (b)(6).

<sup>56</sup> The second section of this report defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of grid security emergency thresholds.

effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event;

or

(B)

(i) a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and

(ii) significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.<sup>57</sup>

Protecting critical and defense critical electric infrastructure against each of these threats will require different types of emergency orders—though some potential orders may be useful against multiple hazards. The threats will also pose disparate challenges for determining whether a grid security emergency is imminent or under way. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the president faces uncertainties about the likelihood and potential consequences of a grid security emergency.

### Geomagnetic Storms as a Possible Initial Focus

Emergency orders for geomagnetic disturbances will entail fewer design challenges than those for cyber attacks and other man-made hazards, and therefore provide opportunities for rapid progress. Geomagnetic disturbance events occur when coronal mass ejections on the sun create geomagnetically induced currents on the earth's surface. These currents can damage unprotected transformers and other grid infrastructure. Compared with the other threats that can trigger grid security emergencies, determining that there is imminent danger of a geomagnetic disturbance event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the president decide whether

to declare a grid security emergency and will provide significant warning before geomagnetically induced currents threaten to damage grid infrastructure.

Industry and government partners can develop emergency orders to take advantage of this warning time. For example, the secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of geomagnetically induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.<sup>58</sup>

A strong foundation already exists for drafting such orders. Studies of the effects of geomagnetic disturbances on the power grid have contributed to a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.<sup>59</sup> Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the federal government to ensure that it has the capability to predict and detect space weather events and the ability to communicate these assessments to public and private sector stakeholders. The order also requires the development of protection and mitigation plans for critical infrastructure and plans for response and recovery if geomagnetic disturbances occur. In addition, the order requires sector-specific agencies to “assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event.”<sup>60</sup>

NERC reliability standards provide an additional cornerstone for developing emergency orders for geomagnetic disturbances. TPL-007-1—*Transmission System Planned Performance for Geomagnetic*

<sup>58</sup> Phillips, “Solar Shield.” See also MISO, *Geomagnetic Disturbance Operations Plan*, 5.

<sup>59</sup> See “NOAA Space Weather Scales,” NOAA; and Kappenman, *Geomagnetic Storms*.

<sup>60</sup> Obama, *Executive Order—Coordinating Efforts*.

<sup>57</sup> 16 U.S.C. § 824o-1, (a)(7).

*Disturbance Events* establishes long-lead geomagnetic disturbance planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat for geomagnetic disturbance events.<sup>61</sup> EOP-010-1—*Geomagnetic Disturbance Operations* also requires reliability coordinators to develop geomagnetic disturbance mitigation plans and operating procedures, including specific actions that transmission operators must take based on predetermined geomagnetic disturbance-related conditions.<sup>62</sup>

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyber attacks and other man-made triggers for grid security emergencies. The sun will not intentionally hide preparations for a geomagnetic disturbance event or “prepare the battlefield” by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data that utility personnel need to maintain situational awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of critical and defense critical electric infrastructure.

The relative ease of drafting orders for geomagnetic disturbances makes such efforts a prime starting point for industry–government collaboration. The North American Transmission Forum, in coordination with the ESCC, is already examining opportunities to develop template emergency orders for geomagnetic disturbance events. But the greater degree of difficulty associated with protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of emergency orders to counter such threats. Instead,

DOE and its industry partners should consider pursuing a multitrack development process: at the same time that they seek rapid progress on emergency orders for geomagnetic disturbances, they should *immediately* accelerate the long-lead work that will be required to counter each of the man-made threats that can trigger grid security emergencies.

### Cyber and Physical Attacks

This report focuses on supporting the development of emergency orders to protect and restore grid reliability against cyber and physical attacks. In doing so, the report follows the lead of the premier electric industry exercise of grid resilience, GridEx. As in previous versions of this exercise series, GridEx IV (conducted in November 2017) employed a scenario based on large-scale, combined cyber and physical attacks against the US electric system by a highly capable adversary.<sup>63</sup> Such combined attacks could pose severe threats to nationwide grid reliability, over and above those created by cyber or physical strikes alone. Grid security emergency orders that can help power companies protect and restore reliability against combined attacks will be especially valuable for national security. Orders and implementation plans that can help counter such severe threats will also be useful in lesser contingencies, including cyber-only strikes.

Current US policy priorities focus on the need to strengthen cyber resilience for the power grid and other critical infrastructure. The US *National Security Strategy* warns that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>64</sup> DOE and its partner utilities should prioritize the development of emergency

<sup>61</sup> NERC, *TPL-007-1*.

<sup>62</sup> The standard, however, does not explicitly lay out what those predetermined conditions should be. See NERC, *EOP-010-1*. For an example of geomagnetic disturbance plans, see PJM, *PJM Manual* 13, 69–71.

<sup>63</sup> GridEx includes participation by over one hundred power companies and other components of the electricity subsector. See NERC, *Grid Security Exercise GridEx IV*, vii.

<sup>64</sup> White House, *National Security Strategy*, 12, 27.



orders to counter such attacks, and supplement the mandatory and increasingly stringent cyber critical infrastructure protection standards, as well as voluntary measures that go above and beyond those NERC requirements.<sup>65</sup>

However, orders can also help build resilience against physical attacks on the grid. Since the coordinated attack on the Metcalf substation near San Jose, California, in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high-powered rifles or other weapons. This includes NERC's *CIP-014-2—Physical Security* standard, which outlines the requirements for protecting grid infrastructure from physical attacks.<sup>66</sup> Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide-area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

An adversary would face greater risks when launching physical attacks than cyber attacks. Blowing up transformers and killing workers who are transporting replacement equipment might rapidly escalate conflict with the United States into larger-scale kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries would hide on utility networks, arming and prepositioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages that last far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk-reward calculus in our favor. If orders can help power companies protect their systems from impending physical attacks, especially in partnership with state and local law enforcement agencies, state National Guard personnel, and other sources of assistance, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Adversaries may also simultaneously employ both cyber and physical attacks. Such combined attacks can synergistically disrupt the grid in ways that cyber or physical attacks on their own cannot. For example, as in the response to cyber attacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.<sup>67</sup> However, physical attacks that destroy critical substation components or target utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

The GridEx IV scenario highlighted the unique challenges posed by combined attacks and opportunities to address them. That scenario also assumed that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging that are far more difficult to counter than in any past US power outage.

This report adopts a similarly severe threat for analyzing possible emergency orders. In particular, the report examines how orders can protect or restore grid reliability against the combined use of cyber weapons, physical attacks, and information

---

<sup>65</sup> NERC has mandatory standards for critical infrastructure protection against cyber threats. See "United States Mandatory Standards," NERC.

<sup>66</sup> DOE, *Quadrennial Energy Review*, 4–34; and NERC, *CIP-014-2*.

---

<sup>67</sup> E-ISAC and SANS-ICS, *Analysis of Cyber Attack*, v.



warfare against critical and defense critical electric infrastructure. Of course, separate types of emergency orders will be required for physical and cyber threats. Orders to deploy specific countermeasures against unmanned aerial vehicle attacks on substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead, utilities can also benefit from examining how emergency orders could help them defeat combined attacks, and how they can integrate both cyber and physical defense operations.

The study does not examine options for developing emergency orders against electromagnetic pulse (EMP) attacks. EMP threats pose a significant potential risk to the grid, and a growing (though still relatively small) number of utilities are hardening their critical systems against EMP effects.<sup>68</sup> DOE's EMP strategy provides a valuable framework and approach for managing the risks that EMP threats pose to the grid and other energy systems.<sup>69</sup> DHS's EMP strategy does the same for a broad range of infrastructure sectors.<sup>70</sup> Industry partners such as the Electric Power Research Institute are also making notable contributions to the shared understanding of EMP effects on the grid.<sup>71</sup> However, significant

research is still required to understand the combined effects of EMP wave components on grid hardware and system-wide operations and for cost-effective mitigation options and preparedness planning.<sup>72</sup> As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

## Thresholds for Declaring Grid Security Emergencies<sup>73</sup>

The FPA authorizes the president to declare a grid security emergency when there is "imminent danger" of an attack or when attacks are already occurring. However, the FPA does not further define imminent, nor provide any criteria to help determine whether the anticipated likelihood of an attack is sufficient to warrant an emergency declaration. As will be discussed below, the FPA provides guidance on the potential severity of imminent or ongoing attacks that would constitute a grid security emergency. However, those guidelines are broad and could be subject to starkly different interpretations in future crises.

Some degree of ambiguity is useful. Preserving wide presidential latitude for declaring grid security emergencies will be essential to deal with unforeseen challenges and to avoid locking US crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicize explicit red lines that would trigger a declaration. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay US defensive measures, including the issuance of emergency orders to safeguard the grid. Adversaries might even seek to spoof the president into declaring a grid security emergency when they had no intention of launching an attack—especially if adversaries believed doing so might prompt the issuance of disruptive emergency orders, crash utility stock

<sup>68</sup> In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to geomagnetic disturbances. The early-time component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See EPRI, *Electromagnetic Pulse and Intentional EMI Threats*, 3-3–3-4.

<sup>69</sup> DOE set strategic goals for addressing EMP threats and created an action plan to meet those goals. DOE, *Electromagnetic Pulse Resilience Action Plan*. The fiscal year 2017 National Defense Authorization Act directed DHS to create a similar strategy, which is currently in draft form. See National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328. The EPRI continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse*.

<sup>70</sup> DHS, *Strategy for Protecting and Preparing*.

<sup>71</sup> EPRI, *Electromagnetic Pulse and Intentional EMI Threats*.

<sup>72</sup> INL, *Strategies, Protections, and Mitigations*.

<sup>73</sup> The analysis in this section builds on the findings of Stockton, "Thresholds."

prices, or incite public panic in ways that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events that emergency orders should be designed to help counter.<sup>74</sup> Federal officials could also find it useful to have decision criteria to help frame their own internal deliberations and recommendations to the president. In an intense crisis, ambiguities in the FPA could fuel disagreements among the president's advisors as to whether the threat of attack was sufficiently severe to declare a grid security emergency. Developing a decision framework to support the declaration process could facilitate consensus-building and provide a structured way to integrate data on attack indicators. However, in adopting such a framework, it would also be prudent to avoid revealing any specific declaration triggers or thresholds for adversaries to exploit in their attack planning.

The section that follows examines two factors that a decision framework might encompass: the likelihood of an attack occurring and its potential consequences. This section also examines how improved information sharing between government agencies and power companies can support these assessments and recommends industry–government consultations in the declaration process that go beyond the existing provisions of the FPA.

### **Determining When Attacks Are Imminent: Criteria for Declaring Grid Security Emergencies**

In key respects, the BPS is under cyber attack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant advanced persistent threats on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS networks, secrete malware

designed to disrupt grid operations, and conduct other malicious activities to prepare for possible attacks on critical system components.<sup>75</sup> PJM Interconnection's former CEO Terry Boston recently stated that the company experiences three thousand to four thousand hacking attempts *every month*.<sup>76</sup> Penetration efforts on a similarly massive scale are likely occurring against BPS entities across the United States. While many of these efforts target information technology systems not directly involved in operating the grid, malware implants on operational technology systems are increasingly frequent and sophisticated.<sup>77</sup> And, as in the case of BlackEnergy and other campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.<sup>78</sup> The net result, according to US director of national intelligence Dan Coats: "Today, the digital infrastructure that serves this country is literally under attack."<sup>79</sup>

Of course, there is a huge gulf between implanting destructive malware on the grid and using that malware to create blackouts. The Trump administration has promised to impose "swift and costly consequences" on foreign governments and other actors who undertake "significant malicious cyber activities" against US critical infrastructure.<sup>80</sup> Attacks that create massive power outages and jeopardize US national security would be especially likely to provoke such a response. However, the president does not need to wait for blackouts to occur before declaring

<sup>75</sup> "Alert (TA18-074A)"; "Alert (TA17-293A)"; Defense Science Board, *Task Force on Cyber Deterrence*, 4; and ICF International, *Electric Grid Security and Resilience*, 19.

<sup>76</sup> Dougherty, "Biggest U.S. Power Grid Operator Suffers Attacks."

<sup>77</sup> "Alert (TA17-293A)"; and "Alert (TA18-074A)."

<sup>78</sup> BlackEnergy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of BlackEnergy inflicted the 2016 blackout on Ukraine. "Alert (ICS-ALERT-14-281-01E)."

<sup>79</sup> Barnes, "Warning Lights."

<sup>80</sup> White House, *National Security Strategy*, 13.

<sup>74</sup> Paradise et al., "ISO-RTO Council Comments," 2.

a grid security emergency. The “imminent danger” of attack is sufficient to declare an emergency and for the secretary to issue orders to help utilities ramp up their defenses.

Implants of new, potentially devastating malware across the electric grid could help the president make such a determination, particularly if other warning indicators suggest that cyber attacks are becoming increasingly likely. The geopolitical context in which cyber attacks might occur provides one such indicator. It is (barely) conceivable that adversaries will launch a “bolt from the blue” attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region and attack the grid to disrupt the deployment of US forces to the region or to achieve other military and political goals.<sup>81</sup> Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause multistate blackouts, should carry greater weight in a crisis environment.

Policy makers should consider developing a framework to assess whether these cyber preparations help justify the declaration of a grid security emergency. The US Office of the Director of National Intelligence (ODNI) has issued a cyber threat framework that could support such development efforts. The ODNI notes that government agencies, academia, and the private sector are using over a dozen analytic models to categorize cyber threats and identify changes in the activities of cyber adversaries. ODNI’s framework is intended to provide a common basis for characterizing threat activity to support analysis and senior-level decision-making.<sup>82</sup> Figure 2 illustrates the cyber threat framework.

<sup>81</sup> The section on preattack grid security emergency declarations examines these national security-related issues and their implications for designing emergency orders.

<sup>82</sup> “Cyber Threat Framework,” ODNI; and ODNI, *Common Threat Framework*, 5.

The initial stage of adversary activity is to prepare for conducting malicious activity. Adversaries then engage and establish presence on targeted systems, allowing them to “operate at will.” In the final stages, attackers seek to destroy grid hardware, software, and/or data, and prepare to conduct follow-on operations as needed to magnify the extent and duration of their disruptive effects.<sup>83</sup>

If adversaries were to suddenly make new moves into the penultimate phase (operate at will) during an intense political crisis or regional confrontation, evidence that they had done so could help the president determine whether attacks were imminent. Other independent sources of data could provide additional context for assessing adversary moves toward more threatening preattack stages. James Miller, former undersecretary of defense for policy, notes that “the United States devotes massive resources to human and technical intelligence collection of our potential adversaries.”<sup>84</sup> Such indicators could contribute to overall assessments of attack imminence.

Policy makers might also supplement the cyber threat framework with specialized attack models for the industrial control systems and other grid components that are crucial for electric system operations. The Industrial Control System Cyber Kill Chain provides an especially promising opportunity to do so. The kill chain identifies the specific sequenced phases that adversaries execute to conduct attacks that inflict predictable physical effects on grid equipment and operations.<sup>85</sup> Stage 1 begins with planning and reconnaissance against

<sup>83</sup> ODNI, *Common Threat Framework*, 13, 16.

<sup>84</sup> Miller, “Cyber Deterrence.”

<sup>85</sup> The Industrial Control System Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin in 2011 to “help the decision-making process for better detecting and responding to adversary intrusions.” The Industrial Control System Cyber Kill Chain tailors that decision-making tool for industrial control system-specific cyber threats and consequences. See Assante and Lee, *Industrial Control System Cyber Kill Chain*.

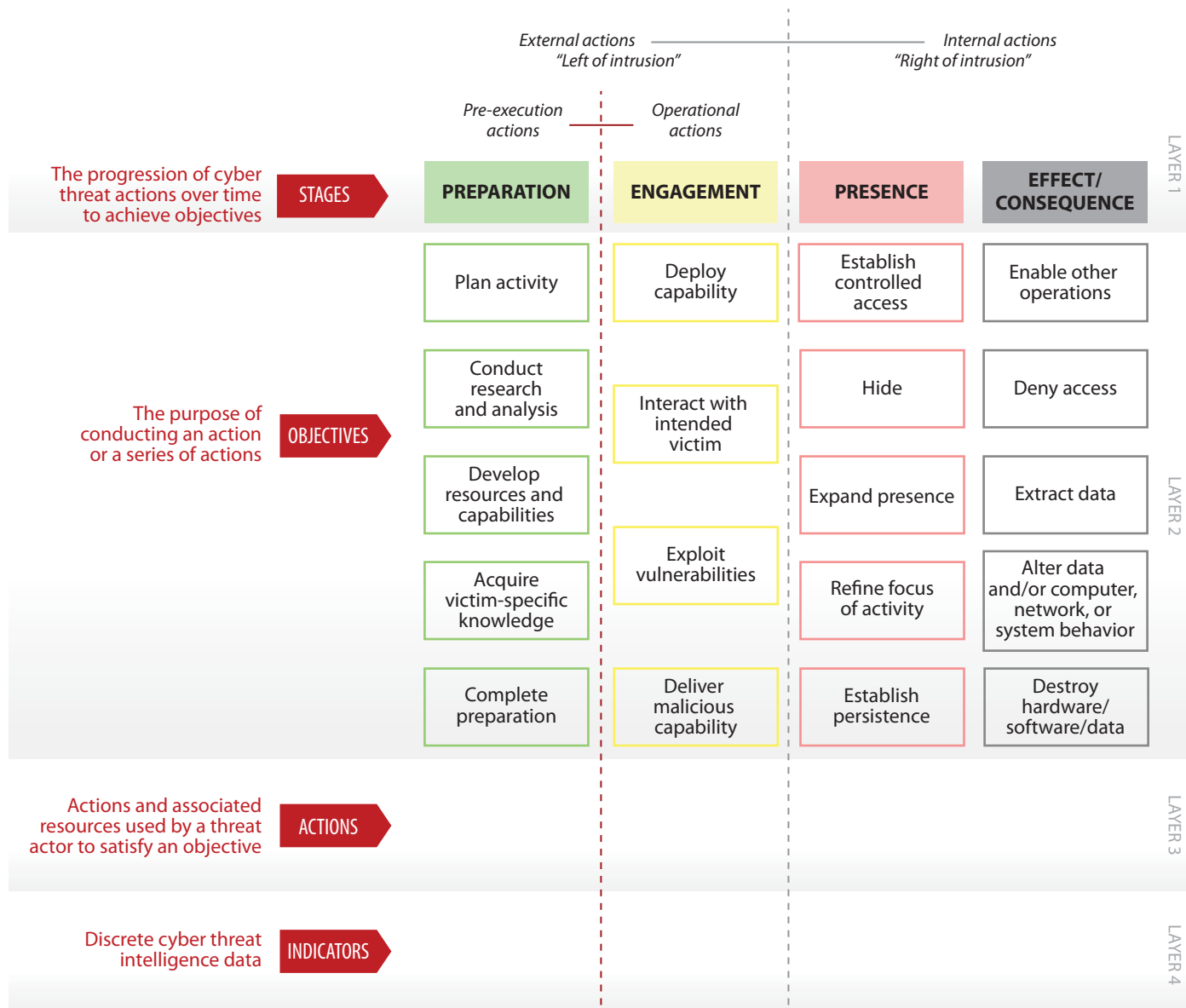


Figure 2. ODNI Cyber Threat Framework

industrial control system networks and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing attack capabilities, and—ultimately—executing the attack. Evidence of an adversary's position along this kill chain could help support decision-making on the imminence of potential attacks, with the final phases posing the most proximate indications that an adversary is poised to strike the grid.

### Potential Attack Consequences

The imminence of an attack provides only one possible criterion for declaring a grid security emergency. A second would be the potential consequences of the attack. Indeed, when Congress defined grid security emergencies in the FPA, legislators established at least implicit, consequence-based thresholds for declaring an emergency. The FPA defines grid security emergencies as occurring when attacks that are imminent or under way "could disrupt the

	General Definition	Observed Action	Intended Consequence
Level 5: Emergency (Black)	<i>Poses on imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons</i>	Effect	Cause physical consequence
Level 4: Severe (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties</i>	Presence	Damage computer and networking hardware
Level 3: High (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>	Engagement	Corrupt or destroy data  Deny availability to a key system or service
Level 2: Medium (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Steal sensitive information
Level 1: Low (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Commit a financial crime
Level 0: Baseline (White)	Unsubstantiated or inconsequential event	Preparation	Nuisance denial of service or defacement

Figure 3. Elements of the Cyber Incident Severity Schema

operation” of devices or networks that are “essential to the reliability of critical electric infrastructure or defense critical electric infrastructure.”<sup>86</sup>

However, the FPA does not clarify the extent of disruption that should trigger the declaration of an emergency. Some grid resilience stakeholders have expressed concern that policy makers might set the threshold too low, and declare grid security emergencies for minor incidents. For example, the ISO/RTO Council proposes that the use of emergency orders in such an emergency “should be reserved for true widespread emergencies.”<sup>87</sup> But

neither Congress nor DOE have yet specified what higher-level thresholds might be appropriate.

One approach to account for the potential consequences of an attack would be to leverage existing federal criteria for categorizing cyber events by the severity of their effects. The definition of “significant cyber incidents” in Presidential Policy Directive 41, *United States Cyber Incident Coordination*, provides a starting point to do so. Under the directive, significant cyber incidents are those that are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or

<sup>86</sup> 16 U.S.C. § 824o-1, (a)(7).

<sup>87</sup> Paradise et al., “ISO-RTO Council Comments,” 2.



public health and safety of the American people.”<sup>88</sup> Policy makers could apply this demonstrable-harm standard to support decisions on whether to declare a grid security emergency. If officials determine that a cyber attack is likely to inflict such harm, their finding would provide a compelling justification for making an emergency declaration.

The December 2016 *National Cyber Incident Response Plan*’s cyber incident severity schema offers a still more detailed basis to assess attack consequences. The schema (Figure 3) serves as “a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments” and agencies.<sup>89</sup> Policy makers could use the schema to help develop consequence-based criteria for declaring grid security emergencies. For example, if assessments suggest that an attack is likely to create a “level 5 emergency,” which poses “an imminent threat to the provision of wide-scale critical infrastructure services, national [government] stability, or to the lives of U.S. persons,” the declaration of a grid security emergency should be near-automatic. Level 4 events would also be very strong candidates for justifying such declarations. However, as with all such criteria, the president should also retain the latitude to make declarations for less severe incidents (for example, the disruption of a cluster of major defense installations).

One advantage of leveraging these government-wide standards is that doing so can help integrate decisions on grid security emergencies into the broader US system for incident response. As officials update the *National Cyber Incident Response Plan* and its supporting severity schema, valuable opportunities will emerge to ensure that grid security emergency declarations and operations are part of a broader, multisector approach to strengthening infrastructure preparedness.

### **Grid-Specific Criteria for Assessing Attack Consequences: Building on Standards for Adequate Levels of Reliability**

If policy makers rely only on general, government-wide decision criteria, they will miss opportunities to take advantage of the electric industry’s standards for assessing the severity of threats to grid reliability. NERC has carefully defined what constitutes adequate reliability for the power grid, as well as the types of large-scale reliability failures that owners and operators need to prevent. If utilities and government agencies have the data and analytic tools necessary to determine whether adversaries’ attacks will create such failures, their assessments could provide valuable input into decisions on declaring grid security emergencies.

The 2003 Northeast blackout spurred NERC’s efforts to define adequate levels of grid reliability and specify the types of system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over wide areas of the United States and Canada, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The 2005 amendments required FERC to certify an electric reliability organization, which will have “the ability to develop and enforce . . . reliability standards that provide for an adequate level of reliability of the bulk-power system.”<sup>90</sup> However, the FPA never defined *adequate level of reliability*; that task was left to the electric reliability organization.

When NERC became the electric reliability organization in 2006, defining the adequate level of reliability was one of its first initiatives. NERC’s board of trustees approved an initial definition for the “characteristics of a system with an adequate level of reliability” in 2008, which was updated in 2013.<sup>91</sup> Three components of NERC’s definition—cascading failures, uncontrolled separation, and instability—are

<sup>88</sup> Obama, *United States Cyber Incident Coordination*.

<sup>89</sup> DHS, *National Cyber Incident Response Plan*, 29–30.

<sup>90</sup> 16 U.S.C. § 824o, (c)(1).

<sup>91</sup> NERC, *Technical Report*, 17.

especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS.<sup>92</sup>

The sections that follow examine these three components, the reliability failures they can entail, and implications for declaring grid security emergencies. Subsequent portions of the report analyze options to develop emergency orders tailored to prevent such failures. However, in grid security emergencies, risks of all three types of failures might emerge in rapid succession and would be inextricably linked.

**Cascading failures.** NERC defines cascading as “the uncontrolled successive loss of system elements triggered by an incident at any location.” Such cascading “results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.”<sup>93</sup> NERC’s definition states that a system is adequately reliable if the system will not experience cascading failures when struck by lightning or affected by other frequent, predictable incidents (i.e., “predefined Disturbances”). But more severe events have caused instabilities that led to cascading in the past and may do so again—especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout illustrates the speed with which failures can cascade. That blackout, which affected approximately fifty million people across the United States and Canada, started with a relatively minor incident. On a hot day in August, multiple 345-kilovolt transmission lines tripped after sagging into overgrown trees. With proper situational awareness, operators might have been able to take actions to handle such a contingency, but failures in

the utility’s control room alarm processor resulted in operators being entirely unaware of the problem. In an unfortunate coincidence, the utility’s reliability coordinator also had computer problems and lacked the visual tools necessary to support grid operators.<sup>94</sup> These failures shifted power flows to a system of 138-kilovolt lines, which were unable to handle the added current flows, and overloaded the last remaining 345-kilovolt path into the area, beginning the major, uncontrollable cascading sequence.<sup>95</sup> This sequence tripped over five hundred generating units and four hundred transmission lines in only eight minutes—with most of these failures occurring *in the last twelve seconds* of the cascade.<sup>96</sup>

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversarial attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying critical generation and transmission nodes; alter protective relay settings so that grid components trip offline (or fail to do so) in ways that intensify the outages; deny grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and take other measures designed to produce cascading failures.<sup>97</sup> Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe—particularly by denying or corrupting situational awareness data.

The imminent danger or occurrence of adversary-induced cascading outages could be a criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt

<sup>92</sup> See section 215 of the FPA, which defines *reliable operation* as “operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” 16 U.S.C. § 824o, (a)(4).

<sup>93</sup> NERC, “Informational Filing,” 1, 7.

<sup>94</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>95</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>96</sup> NERC Steering Group, *Technical Analysis of Blackout*, 109.

<sup>97</sup> Cherepanov and Lipovsky, “Industroyer”; Sistrunk, “ICS Cross-Industry Learning”; “Alert (TA17-163A)”; and Dragos, *CRASHOVERRIDE*, 24.

the operation of grid devices and networks essential to critical and defense critical electric infrastructure—on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

**Uncontrolled separation.** NERC defines uncontrolled separation as “the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss.”<sup>98</sup> Severe events “resulting in the removal of two or more BES elements with high potential to cascade” can produce uncontrolled separation.<sup>99</sup>

Uncontrolled separation almost always occurs in conjunction with cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands that “quickly became unstable after the massive transient swings and system separation” because there was insufficient generation within the islands to meet electricity demand.<sup>100</sup> Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.<sup>101</sup> In the 1982 West Coast blackout, loss of 500-kilovolt lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, dividing the system into four unplanned islands.<sup>102</sup> A similar blackout in the same region in 1996, triggered by multiple major transmission line outages, again separated the Western Interconnection into four electrical islands

“with significant loss of load and generation.”<sup>103</sup> The onset of adversary-induced uncontrolled separation would provide a clear-cut basis for declaring the existence of a grid security emergency, if cascading failures had not already prompted the president to make such a determination.

**Instability.** NERC defines system instability as “the inability of the Transmission system to remain in synchronism . . . characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES.”<sup>104</sup> The BES can experience frequency, voltage, or angular instability—though none should occur during normal operating conditions.<sup>105</sup>

Severe natural hazards and other disturbances can create temporary instabilities. Grid protection systems and operational protocols typically mitigate their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, the transmission system may experience large power swings if BPS generators accelerate or decelerate too much during a disturbance, causing transmission lines to trip and generators to go out of step and trip offline, and resulting in further acceleration and deceleration—or both.<sup>106</sup> Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread cascading failures. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur. Corrupting or disabling protection systems could also make critical grid components vulnerable to physical damage from enemy-induced power surges.

<sup>98</sup> NERC, “Informational Filing,” 6.

<sup>99</sup> NERC, “Informational Filing,” 13.

<sup>100</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 75.

<sup>101</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 104.

<sup>102</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 105.

<sup>103</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 106.

<sup>104</sup> NERC, “Informational Filing,” 6.

<sup>105</sup> NERC, “Informational Filing,” 1–2.

<sup>106</sup> NERC, “Informational Filing,” 6.

Evidence that adversaries were taking preparatory measures to create widespread instabilities could help the president determine that a grid security emergency exists.

However, it may be difficult to predict whether an impending attack will create such failures. The first requirement to do so will be to determine the extent to which adversaries have embedded advanced persistent threats or established other means of attack across the grid—a task that adversaries will complicate by attempting to hide their malware from detection. The next step will be to rapidly characterize these threats, assess the vulnerability of utility systems to them, and predict the consequences for grid reliability if the enemy strikes. Such assessments will also need to account for system-wide effects involving the interaction of multiple adversary-induced disruptions, which may compound and reinforce instabilities in ways that are difficult to predict. PJM Interconnection, LLC, the regional transmission operator for much of the Mid-Atlantic and some neighboring states, recently noted that “additional study is needed to better understand the expected impacts of a large-scale cyber-attack.”<sup>107</sup> Given these challenges, it may be difficult to fully predict the potential impact of cyber attacks on grid reliability until attacks are well under way.

But it could also be risky to wait until attacks are occurring to declare a grid security emergency. In the 2003 Northeast event, for example, cascading blackouts spread across vast areas in seconds. If the president delays declaring a grid security emergency until cascades are under way, emergency orders designed to help prevent their spread may come too late. A better option might be to make an early decision based on imperfect assessments, especially if (as this report recommends) DOE can issue preattack emergency orders that will bolster grid defenses without disrupting normal electric service.

In particular, the president could consider declaring a grid security emergency if (1) an attack appears to be increasingly likely, and (2) assessments indicate that the impending attack may create cascading blackouts or other widespread instabilities. Figure 4 illustrates one option for developing a decision support framework that accounts for the likelihood and potential consequences of an attack. The vertical axis depicts the ODNI cyber threat framework’s four stages of adversary actions, from potential attack preparations to actual strikes against the grid. An adversary’s sudden, large-scale moves up this axis—especially in the context of a severe international crisis—could help the president determine that an attack is impending. The horizontal axis represents the risk that if an attack occurs, the grid will experience cascading failures and other widespread instabilities that would inflict demonstrable harm to national security, the economy, or public health and safety. Attacks that pose little or no risk of cascading blackouts might not warrant the declaration of a grid security emergency.

However, systemic threats to grid reliability are far from the only consequence-based criteria that the president might want to consider. More narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security, such as the National Capital Region, might be sufficient to declare a grid security emergency. Policy makers could develop more refined decision frameworks to account for a broad array of consequence thresholds, as well as further criteria for assessing attack imminence.

## Data Sharing and Consultations with Industry

The electric industry can provide data and analytic support to help the president and other officials decide whether to declare a grid security emergency. Power companies will have direct access to the malware that adversaries implant on their networks, and will be well positioned to assess the potential

<sup>107</sup> PJM, “Comments and Responses,” 35.



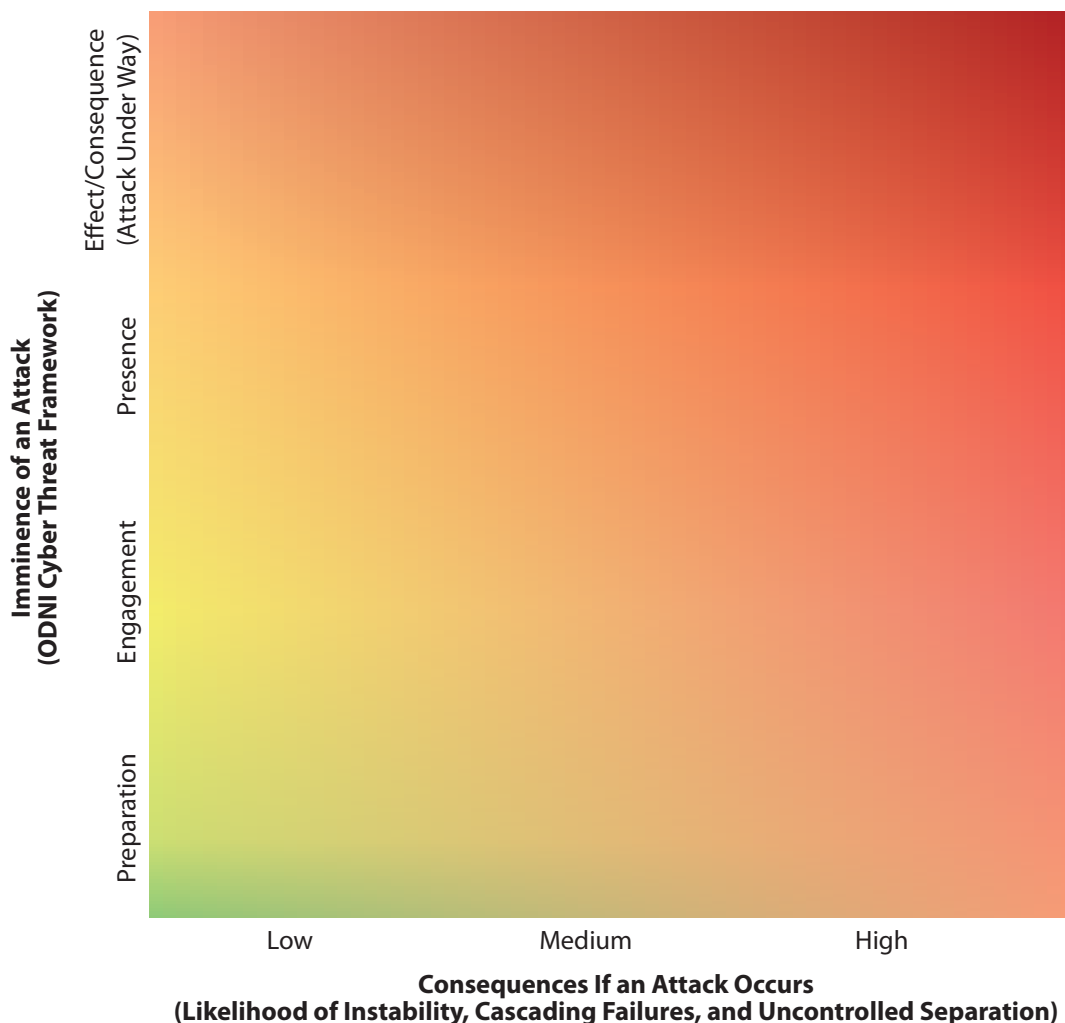


Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies

impact of various attack vectors on their systems and on the grid as a whole.

Government agencies and cyber contractors can help utilities target searches for this malware and provide additional value for the declaration process. If a regional crisis or other geopolitical factors increase the risk of cyber attacks on the grid, agencies should be prepared to ramp up information sharing with BPS entities, especially in terms of specific signatures or other threat indicators to search for in utility networks, logs, and critical equipment.

Industry and government should also explore how ongoing threat detection and analysis initiatives could directly help assess the imminence and

potential consequences of attacks. For example, DOE has projects under way to bolster situational awareness for operational technology networks that could be applied to support such assessments. The department is developing capabilities to monitor traffic on operational technology networks via the Cybersecurity for the Operational Technology Environment project.<sup>108</sup> Other department-funded projects could prove useful for the emergency declaration process as well.<sup>109</sup>

<sup>108</sup> DOE, *Multiyear Plan*, 23.

<sup>109</sup> See, for example, the Containerized Application Security for Industrial Control Systems, Survivable Industrial Control Systems, and Research Exploring Malware in Energy Delivery Systems projects. “Sandia’s Grid Modernization Program



Utilities and DOE might also refine ongoing information sharing initiatives to directly support the emergency declaration process. For example, DOE's Cybersecurity Risk Information Sharing Program is a public-private partnership to build bidirectional situational awareness and facilitate classified and unclassified information sharing.<sup>110</sup> DOE's 2018 cybersecurity plan launched additional activities to advance industry participation in the program, as well as its analytic tools and capabilities.<sup>111</sup> The program is managed by NERC and the E-ISAC, which play an integral role in sharing information and establishing situational awareness within the electricity subsector.<sup>112</sup> In addition, FERC recently issued a proposed directive for NERC to expand reporting requirements for cyber incidents, including for those that "might facilitate subsequent efforts to harm the reliable operation of the bulk electric system."<sup>113</sup> All of these efforts could be integrated to support assessments of the likelihood and potential consequences of attacks.

DHS's May 2018 cybersecurity strategy provides a broader approach to expand information sharing. Most important, the strategy could enable data from other infrastructure sectors to support the declaration process, especially from communications systems and other sectors that support power restoration operations. The strategy also calls for the expansion of automated mechanisms to receive, analyze, and share cyber threat indicators, defensive measures, and other cybersecurity information with critical infrastructure and other key stakeholders.<sup>114</sup>

Such automated sharing mechanisms will be vital to accelerate the identification and assessment of malware that could pose imminent threats to grid reliability. DHS's Automated Indicator Sharing capability "enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed."<sup>115</sup> This bidirectional information sharing will limit an adversary's ability to compromise multiple systems with the same malicious code. The Defense Advanced Research Projects Agency is also working on new technologies to protect the grid. In particular, the agency's Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is working with companies to develop prototype capabilities for improving attack detection, response, and forensics support.<sup>116</sup> Moreover, as automated malware detection and analytic techniques improve, utilities may be able to speed their evaluation of potential intrusions and slash the number of false positives that current detection systems generate.<sup>117</sup> All of these initiatives should be leveraged to help the president determine whether to declare a grid security emergency.

Policy makers should also consider preplanning to consult with grid owners and operators in the declaration process. The FPA leaves the president with sole authority to declare a grid security emergency. If a potential emergency surfaced, the president would almost certainly draw on the expertise and recommendations of the secretary of energy, as well as other members of the National Security Council and supporting agencies. But power companies and their industry organizations will also have perspectives on operational and technical issues that could prove valuable for assessing potential attacks.

---

Newsletter," Sandia National Laboratories; and "REMEDIYS," Cyber Resilient Energy Delivery Consortium.

<sup>110</sup> "Energy Sector Cybersecurity Preparedness," DOE.

<sup>111</sup> DOE, *Multiyear Plan*, 23.

<sup>112</sup> "Electricity Information Sharing and Analysis Center," NERC.

<sup>113</sup> FERC, *Cyber Security Incident Reporting Reliability Standards* (161 FERC ¶ 61,291), 2.

<sup>114</sup> DHS, *Cybersecurity Strategy*, 13.

---

<sup>115</sup> "Automated Indicator Sharing (AIS)," US-CERT.

<sup>116</sup> Douris, "DARPA Research."

<sup>117</sup> Ucci, Aniello, and Baldoni, "Survey on Machine Learning," 1:5; McElwee et al., "Deep Learning"; and McElwee, "Probabilistic Cluster."

Neither the FPA nor the grid security emergency rule explicitly provide for consultations with industry on whether to declare a grid security emergency. The FPA calls for consultations “to the extent practicable” before the secretary issues emergency orders.<sup>118</sup> But there are no equivalent provisions to include industry input in the emergency declaration process.

Industry and government partners should explore options to provide for such consultations, preferably by leveraging existing mechanisms under the ESCC and E-ISAC. As with consultations on issuing orders, urgent circumstances could shorten or preclude opportunities for government dialogue with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of “bolt from the blue” attacks. Nevertheless, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be invaluable for determining whether (and when) to declare a grid security emergency.

## Grid Security Emergency Phases and Order Design Options

DOE and its industry partners should consider designing emergency orders for three potential phases of grid security emergencies. First, if the president determines that there is an imminent danger of an attack, the secretary should be ready to issue preattack orders that help utilities protect grid reliability. Second, once attacks are under way, the secretary could issue orders to reduce the risk of cascading failures or other widespread disruptions of electric service. Third, as utilities begin to restore grid reliability, orders could help utilities replace damaged equipment and counter adversary efforts to disrupt restoration operations.

Orders for each phase of a grid security emergency will differ not only in terms of when the secretary would issue them but also in the degree to which they

will disrupt normal electric service. Some orders, such as staffing up emergency operations centers before an attack occurs, would leave customers unaffected. In contrast, orders for prioritized load shedding could temporarily halt service to many customers—but could also greatly reduce the risk that instabilities will lead to cascading blackouts.

Figure 5 provides examples of orders that vary in the degree of disruption they would inflict on normal service, and also in the way they would meet the phase-specific challenges of grid security emergencies. The analysis that follows examines each of them (and other possible orders) in greater detail.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, emergency orders for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are under way. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies “stop the bleeding” from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are under way.<sup>119</sup> Adversaries may also launch follow-on attacks once utilities begin focusing on restoration. Emergency orders to help utilities repel such attacks could become essential components of the restoration process.

<sup>118</sup> 16 U.S.C. § 824o–1, (b)(3).

<sup>119</sup> In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is fully restored to pre-event conditions) as the “new normal”—characterized by “degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months.” See Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

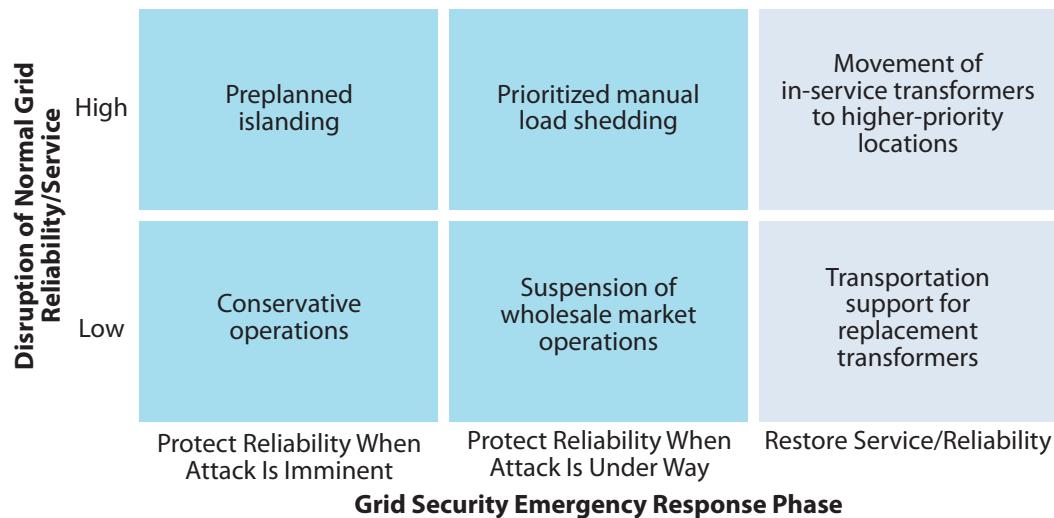


Figure 5. Emergency Order Matrix: Examples of Order Designs

DOE and its partners will need flexibility to deal with the overlapping phases of grid security emergencies. Nevertheless, being able to categorize potential orders in terms of when they would likely be issued and which phases of emergency operations they could support can help establish a systematic process for developing orders.

Creating emergency orders for all three phases can also help utilities and DOE integrate the orders into seamless, multiphase operational plans for grid security emergencies. As intense regional crises or other events elevate the risk of attacks on the grid, it will be prudent to preplan for the issuance of emergency orders for multiple grid security emergency phases. Orders for preattack measures such as conservative operations would be issued first if attacks are deemed imminent. At the same time, however, DOE and the utilities subject to emergency orders should be using any available warning time to prepare for the issuance and implementation of orders for the midattack and restoration phases.

## Preattack Options

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal

with these ambiguities is to delay the declaration of a grid security emergency until blackouts begin; doing so would forego the benefits of issuing preattack emergency orders. It may be possible to develop orders that will offer significant benefits if adversaries strike yet also have little or no impact on normal service—thereby offering “no-regrets” options to employ when the likelihood of an attack remains uncertain. Industry and government partners should also explore options for the preattack phase that would be more disruptive but also offer potentially far-reaching benefits. These two options occupy the left-hand column in Figure 5.

Conservative operations that utilities employ against natural hazards provide a model for protecting the grid in ambiguous preattack situations. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects and prepare for possible response and restoration operations if grid infrastructure is damaged.<sup>120</sup> For

<sup>120</sup> Conservative operations are not defined in the NERC glossary of terms. However, many reliability coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken to “implement

example, reliability coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.<sup>121</sup> Power companies may also cancel noncritical generation and transmission maintenance activities; reduce transfer limits to give the transmission system extra “slack”; and staff their backup control centers, critical BPS substations, and other vital facilities to set the stage for emergency operations as hurricanes approach.<sup>122</sup>

A defining feature of these frequently used conservative operations is that they do not disrupt normal service to customers. Their negligible service impact makes them more viable to implement when the storm’s path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the US coast. Instead, they provide a wide “cone of uncertainty” that becomes increasingly narrow as the hurricane approaches. Utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other conservative operations. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these operations do not affect normal service to customers enhances the willingness of utility leaders to order their implementation while the storm track remains uncertain.

---

additional actions to ensure the BES remains reliable in the face of the additional threats” when “events, conditions, or circumstances may put the Bulk Electric System (BES) at an increased level of risk, compared to normal operating conditions.” See PJM, “Conservative Operations,” 3. Similarly, the Western Electricity Coordinating Council, defines conservative systems operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets “are restricted and managed in order to maintain or restore reliability of the power system from the negative influence of a triggering event or condition.” See Western Electricity Coordinating Council, “Conservative System Operations,” 4.

<sup>121</sup> PJM, “Conservative Operations,” 3.

<sup>122</sup> PJM, “Conservative Operations,” 9.

Industry and government partners should borrow from this model to develop orders for preattack conservative operations against cyber and/or physical attacks. Some have already begun to do so. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting conservative operations to meet the specialized challenges posed by cyber and physical threats.<sup>123</sup> This preparation will be extremely helpful as potential attacks loom. As a regional confrontation or other precipitating crisis intensifies, it is conceivable that the US intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. However, it is much more likely that ambiguities will persist about whether the adversary will actually attack and risk a devastating US response. To ensure that sufficient time is available to implement conservative operations, the secretary may need to order the initiation of such measures when enemy intentions remain uncertain—and when warning indicators may turn out to be false.

Many of the conservative operations that will bolster resilience against adversary attacks would be similar to those developed for natural hazards. For example, preattack emergency orders might direct BPS entities to increase generation reserves and/or re-dispatch resources out of least-cost operations. Other orders might be threat specific: for example, to intensify scrutiny of operational technology networks for malware and implement government-vetted counter-measures in ways that give utilities sufficient latitude to account for their unique system characteristics.

The common denominator for all such options: if the secretary issues orders for BPS entities to adopt conservative operations and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented the orders.

---

<sup>123</sup> See, for example, PJM, *PJM Manual* 13, 73; Lucas, “Conservative Operations”; and SERC, *Conservative Operations Guidelines*.



However, because so many utilities already have robust plans and capabilities to protect their systems from imminent threats, close government–industry coordination will be required to ensure that emergency orders actually assist grid defense rather than function as speed bumps or useless distractions. Reliability coordinators and other grid operators serve as the pointy end of the spear for protecting grid reliability. Mandatory NERC standards require BPS entities to maintain voltage stability, automatic load shedding schemes, and contingency reserves for disturbances.<sup>124</sup> NERC standards also require transmission operators to “develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area.”<sup>125</sup> Balancing authorities have similar requirements to manage generating and demand-side resources in their service areas.<sup>126</sup> These plans are exercised, tested, and frequently updated to bolster their effectiveness for actual emergencies. While many of NERC’s mandatory standards apply when disturbances begin to occur, BPS entities are spring-loaded to implement conservative operations the moment potential hazards begin to emerge.

If major grid disruptions occur, BPS entities will not sit on their hands and wait for the president to declare a grid security emergency and the secretary to issue emergency orders. Indeed, DOE does not contemplate that they will. In the final grid security emergency rule, the department states that the declaration of a grid security emergency “does not preclude electric utilities from taking time-sensitive action to secure the safety, security, or reliability of the electric grid prior to the issuance of an emergency order.”<sup>127</sup>

DOE and its partners can design emergency orders to help supplement and support such industry-led operations. For example, government agencies may acquire highly classified indicators that an attack is imminent. Declaring a grid security emergency and issuing emergency orders for conservative operations could ensure that utilities bolster their preparedness against such attacks on a consistent, nationwide basis, including those utilities that had not yet identified a need to act. Orders to help power companies ramp up and target searches for specific types of malware could supplement utilities’ defensive operations as well. The secretary might also issue orders to ensure that such industry operations benefited from the FPA’s regulatory protections and cost-recovery provisions.

### More Disruptive Preattack Options

Many utilities are also prepared to take pre-event emergency measures that will significantly disrupt normal electric service, yet also offer benefits far beyond those that conservative operations can provide. For example, power companies can selectively halt electric service on warning of catastrophic storm surges. If seawater hits systems that are still carrying electricity, transformers and other difficult-to-replace grid components will suffer catastrophic physical damage. In 2012, weather forecasters warned that Superstorm Sandy might produce storm surges that would inundate critical substations and underground electrical equipment in lower Manhattan. Consolidated Edison’s team made the politically difficult decision to prevent such damage by preemptively cutting of power to the area. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.<sup>128</sup> Moreover, Consolidated Edison limited the shutdown’s disruptiveness by notifying customers hours earlier that the utility might halt service and by already having plans in place to prioritize the

<sup>124</sup> See, for example, NERC, *VAR-001-4.2*; NERC, *Standard PRC-006-3*; NERC, *PRC-010-2*; and NERC, *BAL-002-2(i)*.

<sup>125</sup> NERC, *EOP-011-1*, R1.

<sup>126</sup> NERC, *EOP-011-1*, R2.

<sup>127</sup> DOE, “RIN 1901–AB40,” 1177.

<sup>128</sup> Miller, “Con Edison Shuts off Power.”



restoration of service to hospitals, water-pumping stations, and other critical facilities.<sup>129</sup>

BPS entities continue to use “shutdown on warning” as an effective tool to avoid equipment damage against severe weather and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent equipment damage and speed up restoration. Generation owners similarly chose to shut down or evacuate some generating units in the storm’s projected path.<sup>130</sup>

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and heating and air conditioning systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

DOE and its electricity subsector partners should consider developing emergency orders that offer a similar set of risks and rewards. However, doing so will entail problems beyond those associated with protecting the grid against natural hazards. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an adversary will actually pull the (cyber) trigger and whether attacks are likely to cause demonstrable harm to the US economy, national security, or public health and safety. Measures developed for natural hazards may also offer uncertain benefits against imminent cyber and physical attacks. For example, further analysis will be required to determine whether and how preattack grid shutdowns might help counter specific cyber threats, including attacks that disable

protection systems to facilitate equipment-damaging power surges.

Other disruptive emergency orders could counter a broader range of threats but entail major (and perhaps insurmountable) problems for nationwide employment. The upper left-hand box in Figure 5 offers a prime example of such options: preplanned power islanding. Microgrids offer the most familiar means of establishing power islands.<sup>131</sup> A growing number of military bases, universities, and major hospitals have sufficient generation and other electric infrastructure on-site so that if adversaries black out the surrounding grid (or pose an imminent danger of doing so), those facilities can separate from the grid and operate independently as power islands.

However, microgrids do not offer “bulletproof” power resilience. Cyber adversaries are sure to treat on-base electric infrastructure, including renewable generation assets, as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas-fired generators, the power they provide is only as resilient as the gas transmission and distribution systems that supply them—and cyber threats to natural gas systems are rapidly escalating.<sup>132</sup> Moreover, building microgrids requires extensive investment in grid infrastructure. Investment demands will be especially heavy if installations want to serve not only the critical loads within their perimeters but also the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to building microgrids, power companies are also analyzing ways to establish emergency power islands with less infrastructure investment. One particular option being explored by GridEx participants is to preplan to establish large

<sup>129</sup> DiSavino and Sheppard, “ConEd Cuts Power.”

<sup>130</sup> NERC, *Hurricane Harvey*, v.

<sup>131</sup> DOE’s definition of microgrids: “A microgrid is a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously.” “The Role of Microgrids,” DOE.

<sup>132</sup> DOE, *Quadrennial Energy Review*, 7-7; and Parfomak, *Pipelines*, 2-3.

power islands by using existing grid infrastructure within their boundaries. Utility personnel have noted that they might be able to use legacy balancing areas as a starting point to establish island boundaries. On warning of an imminent attack or under other extraordinary circumstances, utilities would separate a power island from the surrounding grid and operate independently to serve critical loads within it. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, preplanned islands might become a hedge against cascading failures and uncontrolled separation.

In practice, preplanned islanding will be practical only if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for preplanned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands to enable them to function independently of the grid. Moreover, standing up islands would severely disrupt day-to-day service for noncritical customers and create instabilities for surrounding systems that could produce additional service disruptions. Accordingly, preplanned islanding might be considered a “huge-regrets” emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created.

DOE and its industry partners should also consider developing preattack emergency orders that fall between the two extremes of no-regrets options and highly disruptive measures. For example, to avoid remote execution of destructive malware on utility networks, orders might direct utilities to disconnect their systems from the internet. Utilities could also take additional measures to isolate or compartmentalize all control systems. Implementing these

measures would curtail potential attack vectors, but would do so at a price. Disconnecting from the internet would hobble wholesale market operations, disable email as a basic communications tool, affect an entity’s access to other means of communications (i.e., E-ISAC and DOE portals), impact an entity’s ability to comply with regulatory requirements, and produce other undesirable consequences. Any unexpected challenges in isolating or compartmentalizing the control systems that are critical to the functioning of the grid could also jeopardize normal service. Nevertheless, if industry and its government partners can preplan to anticipate and overcome these challenges, even highly disruptive preattack options may be useful to protect the grid from cascading failures.

## Extraordinary Measures when Attacks Are Occurring

Emergency orders when attacks are underway can help utilities prevent widespread instabilities, cascading failures, and uncontrolled separation. Under the auspices of the ESCC, utilities and their resilience partners are already developing “extraordinary measures” to operate the grid if adversaries disable or corrupt SCADA (supervisory control and data acquisition) systems, state estimators, and other operational technology hardware and software components on which utilities typically rely.<sup>133</sup> For example, the North American Transmission Forum is leading an initiative on supplemental operating strategies to help power companies manually cope with the loss of energy management systems and/or SCADA across a large geographic footprint.<sup>134</sup>

---

<sup>133</sup> These extraordinary measures include resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary backup systems, and development of supplemental operating strategies use in “degraded states.” See “ESCC: Electricity Subsector Coordinating Council,” ESCC.

<sup>134</sup> Galloway, “Advancing Reliability and Resilience of the Grid,” 2.

These industry efforts provide a basis to develop grid security emergency orders for extraordinary measures when attacks are under way. So, too, do existing BPS emergency operating plans, capabilities, and operational requirements to manage the grid instabilities. Options for such orders vary in terms of the disruption they would inflict on normal grid operations.

Figure 5 provides an example of a low-disruption order for this phase: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate needs or for the next day). These entities have taken extensive measures to keep market functions separate from their operational control of the grid. Many entities also have mechanisms in place to operate when markets are temporarily suspended. Over extended periods, however, cyber attacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, undercut the valuation of power companies on Wall Street, and magnify the damage to the US economy that attacks on the grid will create.

Regional transmission organizations are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the transmission operator<sup>135</sup> for the Mid-Atlantic and other US regions, has called for the development of mechanisms to permit “nonmarket” operations in extreme circumstances.<sup>136</sup> A number of options exist to provide for such operations. For example, if the secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell

power at a fixed price predetermined by DOE.<sup>137</sup> Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high-benefit/low-disruption emergency orders, including orders for maximum power generation when attacks are under way, will also fall into this category.<sup>138</sup>

Industry and government partners will also need to develop more disruptive emergency orders that can protect grid reliability in extraordinary circumstances. One option to do so involves operating an area in a generation-deficient state for a prolonged period, supported (when practical) by power imported from neighboring regions. The top center box of Figure 5 provides another prominent example: prioritized manual load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by selectively shedding load and implementing rotating blackouts.<sup>139</sup>

A failure to shed load contributed to the cascading failures in the major 2003 blackout. After-action reports from that event found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission

<sup>135</sup> The NERC glossary defines *transmission operator* as “the entity responsible for the reliability of its ‘local’ transmission system, and that operates or directs the operations of the transmission Facilities.” *Transmission operator area* is defined as “the collection of Transmission assets over which the Transmission Operator is responsible for operating.” See NERC, *Glossary*.

<sup>136</sup> PJM, “Comments and Responses,” 6, 39–40.

<sup>137</sup> Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. PJM, “Comments and Responses,” 39.

<sup>138</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual 13*, 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see MISO, “MISO January 17–18 Maximum Generation Event Overview.”

<sup>139</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 11.

lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. A US–Canada task force found that “timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio.”<sup>140</sup> In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.<sup>141</sup>

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for transmission operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation for building emergency orders to reduce the risk that physical and cyber attacks will create cascading blackouts.

One way to shed load would be to order power companies to execute rotating blackouts. In such controlled outages, grid operators interrupt service on a rotating basis to sequential sets of distribution feeders for limited periods (typically twenty to thirty minutes).<sup>142</sup> Grid operators employed rotating blackouts to help protect grid reliability during the “Big Chill” that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT’s rotating blackouts during the event affected a total of 4.4 million customers.<sup>143</sup> The temporary blackouts were no doubt disruptive. However, by reducing the risk of cascading failures, those

outages offered compelling system-wide benefits for protecting reliability.

But rotating blackouts will not offer the best option for load shedding in all grid security emergencies. In the event of a massively disruptive attack, an emergency order might require utilities to shed load without implementing rotating blackouts, because such rotating outages could introduce unacceptable reliability risks during a chaotic and rapidly changing situation. As an alternative, utilities can implement “brownouts”: that is, conduct voltage reductions to maintain a continual balance between supply and demand within a balancing area.<sup>144</sup> However, brownouts and rotating blackouts share a serious limitation: they affect all customers equally. But not all customers will be equally important in a grid security emergency. DOE and industry will need orders and implementation plans for manual, prioritized load shedding, so utilities can focus on sustaining power flows to hospitals and other critical loads while also reducing the risk of cascading power failures. NERC already requires BPS entities to have plans for both automatic and manual load shedding.<sup>145</sup> Utilities and DOE should use these requirements as the starting point to design emergency orders for extraordinary measures that would supplement what BPS entities are already prepared to do to if major instabilities occur.

## Emergency Orders to Support Power Restoration

The rightmost column in Figure 5 provides the third category for emergency orders: those that can help grid owners and operators restore power after widespread

<sup>140</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 147.

<sup>141</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 77.

<sup>142</sup> NERC, *Reliability Terminology*, 1.

<sup>143</sup> FERC and NERC, *Restoration and Recovery Plans*, 61.

<sup>144</sup> NERC, *Reliability Terminology*.

<sup>145</sup> NERC standards currently emphasize automatic load shedding to protect grid reliability. See NERC, *Standard PRC-006-3*; and NERC, *PRC-010-2*. However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing emergency orders to prevent or mitigate cascading failures. See NERC, *EOP-011-1*.



outages occur. In past cascading failures of the US electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days (and in some cases much less time) because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators, transmission lines, and other system components are designed to trip offline when instabilities occur, thereby protecting them from damaging power surges—and leaving them available to help rapidly reestablish the flow of power.<sup>146</sup> However, if cyber or physical attacks destroy critical system components, requirements to repair or replace such assets could greatly lengthen and complicate the restoration of service. Emergency orders can support restoration operations and better align them with national-level priorities.

Emergency orders for the restoration phase can also account for the risk that adversaries may continue their attacks as power companies begin to restore service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to US military bases and other vital facilities and to seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeting power restoration operations can help adversaries achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply. Risks of reattack should help drive the design of restoration-phase emergency orders.

Advanced persistent threats hidden in utility networks will pose especially significant challenges for restoration. This malware may enable adversaries to conduct recurring attacks based on timing or network

conditions. Unless utilities thoroughly eradicate such malware, repeated outages could impede restoration operations and put the grid at sustained risk of cascading failures.<sup>147</sup> Physical attacks against restoration personnel and replacement equipment in transit would pose additional problems. Grid security emergency orders can help utilities restore electric service even if they remain “under fire” from cyber and kinetic weapons.

Such orders will differ in the degree to which they could alter existing utility plans to restore power. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks, and barges) from where power companies store them to where they are needed as replacements.<sup>148</sup> Subsequent portions of this report examine how DOE could collaborate with other federal agencies and state and local officials to waive transportation regulations and bolster security support for such operations. The secretary could also issue orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, ports, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these prioritized customers. Emergency orders can help incorporate other national security-related assets that utility plans do not typically include, such as components of the defense industrial base essential for resupplying US forces abroad.

DOE and its industry partners should also create template emergency orders for in extremis restoration operations that would more sharply depart from existing industry plans and procedures. The upper right-hand box of Figure 5 offers an example

---

<sup>146</sup> NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, 1.

<sup>147</sup> Homeland Security Advisory Council, *Final Report*, 7.

<sup>148</sup> DOE, *Strategic Transformer Reserve*, 12–13.



of one such option. If adversaries damage or destroy an extraordinarily large number of transformers, the secretary might order utilities to remove surviving in-service transformers in the same voltage class from their substation and transport them to serve vital national security facilities in the National Capital Region or other areas. Orders of this kind could create severe disruptions in existing service. They might even impede system restoration if utilities and their government partners have not adequately prepared to account for challenges regarding transformers' technical specifications and the BPS's overall configuration. However, if these challenges can be addressed, the benefits might be greater still for helping the United States defeat its adversaries.

Other in extremis orders could help utilities operate the grid if equipment damage is so extensive (or reattacks are so effective) that full system restoration will require many weeks or even months. The FERC/NERC study on severe impact resilience (May 2012) found that coordinated cyber and physical attacks may force the grid into a "new normal" state of "degraded planning and operating conditions" that could last for months or years, including reduced generation and transmission resources and planned and unplanned rotating blackouts.<sup>149</sup> DOE and power companies should consider how emergency orders and supporting regulatory waivers might help electric utilities serve priority loads and accelerate restoration under new normal conditions.

One option to do so is to preplan for the waiver of selected reliability standards. The *Severe Impact Resilience* study recognized that catastrophic events could "put entities in a position where they cannot comply with all standards." However, in part due to the difficulty of predicting the circumstances that entities will face, the study recommended against preplanning for waivers. Instead, the study proposed relying on entities to "do the right thing" for reliability

and public safety" and self-report violations as circumstances permit.<sup>150</sup>

NERC should reconsider this conclusion in light of the secretary's new grid security emergency authorities and the waiver provisions they entail. FERC, NERC, and their industry and government partners should identify specific regulatory waivers and related measures that could provide the basis for utilities' contingency planning for new normal operations.

One such option lies in reliability standards for managing unforeseen contingencies. Currently, NERC standards require BPS entities to operate in an N-1 state: that is, they must be able to sustain service even if they suffer the most severe single contingency (such as the loss of a single critical line, transformer, or generator) possible in their system.<sup>151</sup> Operators may be required to shed load prior to any contingency to maintain the N-1 state. These requirements apply during normal day-to-day operations as well as during system restoration.

Returning to an N-1 state in the face of coordinated cyber and physical attacks is likely to be a lengthy process involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. To help enable utilities to serve critical facilities during such sustained events, the secretary might issue emergency orders that explicitly allow utilities to function in an N-0 operating state (as long as doing so did not risk causing cascading failures or equipment damage).<sup>152</sup>

Issuing such orders could entail important benefits. Operating at N-0 would give utilities greater operating flexibility and ensure that entities can continue to serve as much load as possible during a grid security

<sup>149</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

<sup>150</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 17.

<sup>151</sup> NERC, *BAL-002-2(i)*, requirement R2; NERC, *TOP-001-3*, R12 and R14; and NERC, *IRO-008-2*, R5 and R6.

<sup>152</sup> For N-0, all elements must be within thermal and voltage limits prior to any contingency.

emergency, including military installations and other priority customers. Unlike under N-1 operations, entities would be required to shed load only prior to any contingency for the most severe single contingencies if any of those single contingencies would cause cascading failures, or after a contingency that required load shedding to eliminate overloads or low voltage.

But operating at N-0 would also entail significant risks. N-1 standards exist for compelling reasons: they help protect grid reliability against severe contingencies. Deviating from N-1 requirements will create greater risks of causing further blackouts in new normal conditions. Moreover, N-0 operations would require even greater coordination among BPS entities (including reliability coordinators, transmission owners, and local control centers), as a single outage could result in equipment overloads or voltage violations and require extraordinary mitigation measures. Accordingly, this option will be feasible only if DOE partners with FERC, NERC, and entities to fully understand and mitigate such risks, as well as maximize the potential benefits of N-0 operations for serving critical national security-related loads.

## Additional Emergency Order Design Parameters and Supporting Initiatives

Adversaries will attempt to black out the US grid to achieve their broader political, economic, and military objectives in a conflict. Government agencies and the electricity subsector should design emergency orders to help prevent attackers from accomplishing their objectives, and—ideally—to help deter them from attacking at all.

However, deterring and defeating attacks on the grid will require resilience improvements beyond the electricity subsector. Attackers may simultaneously strike electric and communications systems to both disrupt the grid and impede the issuance and

implementation of emergency orders. Adversaries may also seek to incite public panic through social media and other information warfare operations to advance their broader political objectives. Countering such efforts will require unprecedented collaboration among utilities, government agencies, media, and the broader telecommunications sector.

Designing and implementing emergency orders to blunt attacks by Russia, China, and other potential high-capability adversaries will place extraordinary burdens on electric utilities—burdens that few ratepayers and utility investors will be eager to bear on their own. To help power companies meet these challenges, it will be essential to fully leverage the regulatory waiver and cost-recovery provisions of the FPA, and examine whether Congress should expand these provisions as threats continue to intensify.

## Deterring and Defeating US Adversaries

The US *National Security Strategy* emphasizes that cyber threats to US critical infrastructure are becoming increasingly severe. In particular, the strategy notes that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>153</sup> Pairing cyber attacks with coordinated physical strikes against transformers and other critical grid infrastructure would exacerbate these disruptive effects.

The strategy identifies two primary means for deterring catastrophic attacks, both of which can be supported by emergency orders and implementation plans:

- (1) Convince adversaries that they will suffer “swift and costly consequences” if they strike the grid or other US targets, and that the United States “can and will defeat them” if deterrence fails.<sup>154</sup>

<sup>153</sup> White House, *National Security Strategy*, 13, 28.

<sup>154</sup> White House, *National Security Strategy*, 28.

- (2) Strengthen infrastructure resilience to create “doubt in our adversaries that they can achieve their objectives” if they do attack (i.e., deterrence by denial).<sup>155</sup>

### **Deterrence through Cost Imposition: Protecting Defense Critical Electric Infrastructure**

In amending the FPA, Congress placed a particular emphasis on the need to protect the reliability of defense critical electric infrastructure (i.e., grid components that serve military bases and other facilities “critical to the defense of the United States” and vulnerable to the disruption of grid-provided electricity).<sup>156</sup> Emergency orders to protect such infrastructure can help ensure that US bases have the power they need to respond to attackers. But prioritizing defense installations for support in grid security emergencies will require deeper analysis of US deterrence requirements, given DOD’s growing dependence on civilian assets and functions to execute defense missions. Deterrence by cost imposition will also depend on convincing potential adversaries that the United States will be able to identify them as the perpetrators of attacks on the grid. DOE and its industry partners should explore how emergency orders can facilitate attack attribution, as well as provide broader support for the credibility of the US deterrence posture.

A relatively small number of military bases are responsible for inflicting unacceptable costs on potential adversaries. The US Defense Science

Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of US strike systems (cyber, nuclear, and nonnuclear) and supporting infrastructure to ensure “that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks.”<sup>157</sup> Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which US strike systems rely and ensure that they have reliable power even in extended conflicts.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The strategy emphasizes that “we must convince adversaries that we can and will defeat them—not just punish them if they attack the United States.”<sup>158</sup> Defeating adversaries in regional contingencies in the South China Sea, the Baltics, or other potential conflict zones will place special burdens on US grid resilience. US capabilities to conduct operations abroad are increasingly dependent on domestic military and civilian assets. In particular, a vast array of US defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy, operate, and sustain US power projection forces for regional conflicts.

This dependence makes the grid a prime target for attack. The DOD *Mission Assurance Strategy* notes that adversaries may seek to disrupt power projection capabilities by attacking the domestic infrastructure systems on which they depend. In particular, the strategy warns that “potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting

<sup>155</sup> White House, *National Security Strategy*, 13, 28. The literature on security studies defines deterrence by denial in a variety of ways. This report follows the definition used in the *National Security Strategy*, which is consistent with the definition employed in the Obama administration’s deterrence policies. See Lynn, “Defending a New Domain.” For broader studies of deterrence by denial, and critiques of the way in which the strategy employs the term, see Fischerkeller and Harknett, “Deterrence Is Not a Credible Strategy”; Mitchell, “Case for Deterrence by Denial”; Gerson, “Conventional Deterrence,” 40; and Nye, “Deterrence and Dissuasion,” 56–58.

<sup>156</sup> 16 U.S.C. § 8240–1, (a)(4).

<sup>157</sup> Miller and Gosler, “Memorandum.” See also pp. 3, 6–7, 11–12, and 17–18 of the report.

<sup>158</sup> White House, *National Security Strategy*, 28.

critical defense and supporting civilian capabilities and assets,” including the US power grid.<sup>159</sup>

Ensuring the availability of resilient power for ports and other civilian assets essential for power projection will require emergency orders to serve an expanded set of customers, far beyond those responsible for strike operations. These orders will also need to encompass a much larger array of defense critical electric infrastructure owners and operators.

Electric companies and defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds from separate high-voltage transmission substations to serve defense installations provides a valuable means of strengthening resilience against physical attacks.<sup>160</sup> Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.<sup>161</sup> Utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as power islands independent of the surrounding grid.<sup>162</sup>

While valuable, these initiatives do not eliminate the need to develop national defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases and will not necessarily provide resilience against cyber attacks (since even redundant feeds may share common cyber vulnerabilities). Emergency generators will break down in long-duration outages. Moreover, resupplying them with fuel will become increasingly difficult at installations that lack massive storage

tanks. Large-scale microgrids for islanded operations can provide more resilient power. DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction and scale them to serve infrastructure loads outside the base that are essential for on-base operations. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for war fighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, including the intermodal transportation systems that help deploy and sustain US forces abroad.

DOE and its industry partners can design emergency orders to support US deterrence credibility and power projection capabilities far more quickly and with less infrastructure investment. However, for utilities to implement these orders, they must first know which customers are of the highest priority for sustaining and restoring service when enemies strike. Section 215A of the FPA provides the ideal starting point develop and share such data. The act requires the secretary of energy, in consultation with other federal agencies and grid owners and operators, to identify and designate “critical defense facilities” in the forty-eight contiguous states and the District of Columbia that are “(1) critical to the defense of the United States; and (2) vulnerable to a disruption of electric energy provided to such facility by an external provider.”<sup>163</sup> Congress’s definition of defense critical electric infrastructure also helps guide implementation of that requirement. Such assets include “any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]” as a critical defense facility, “but is not owned or operated by the owner or operator of such facility.”<sup>164</sup>

<sup>159</sup> DOD, *Mission Assurance Strategy*, 1.

<sup>160</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39.

<sup>161</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 40.

<sup>162</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39. See also Van Broekhoven et al., *Microgrid Study*; and Marqusee, Schultz, and Robyn, *Power Begins at Home*, 13–15. A number of “islandable” microgrid projects are under way at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See McGhee, “EEI Executive Advisory Committee,” 4; and Kaften, “DoD Tests Energy Continuity.”

<sup>163</sup> 16 U.S.C. § 824o–1, (c).

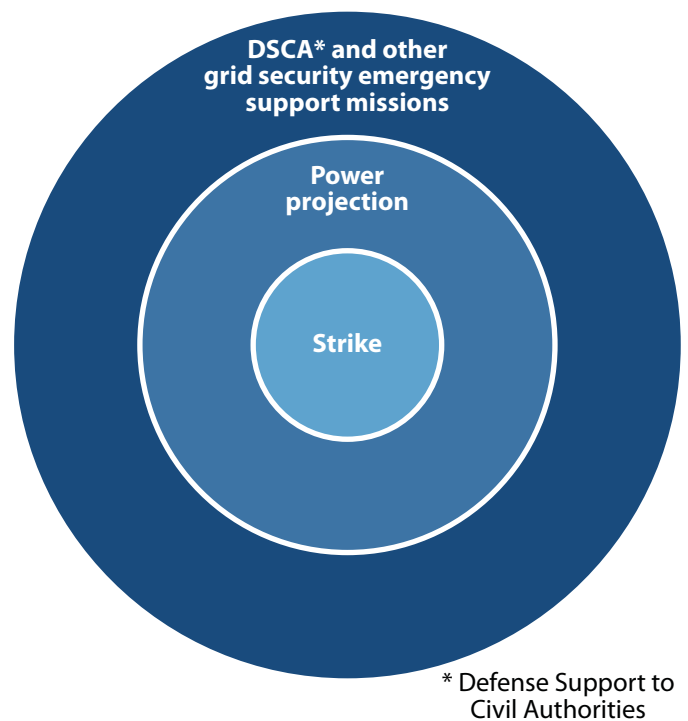
<sup>164</sup> 16 U.S.C. § 824o–1, (a)(4).



DOE is already working with DOD to identify defense critical electric infrastructure and the installations this infrastructure serves. DOD has a well-established, continuously updated list of critical military bases and other DOD assets to support this identification process.<sup>165</sup> However, deterrence and power projection will also depend on sustaining electric service to a diverse array of ports, transportation systems, and other civilian-owned infrastructure. Figure 6 illustrates how DOE, DOD, and their partners might categorize all such defense-related assets and the defense critical electric infrastructure that grid security emergency orders should help protect.

At the innermost core lie those installations and supporting infrastructure capable of inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital. Protecting the reliability of the defense critical electric infrastructure on which they depend should be the top nationwide priority for developing emergency orders and company-specific implementation plans.

The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining these assets abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the US grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. DOD is in the process of identifying the specific facilities and supporting infrastructure that are required to help execute operational plans around the globe.<sup>166</sup> The department also has well-established criteria and assessment methods to prioritize these supporting assets for risk mitigation.<sup>167</sup> DOD and DOE should use these tools to identify the broader set of defense critical electric infrastructure needed for deterrence



**Figure 6. Categories for Protecting Defense Critical Electric Infrastructure**

and to help power companies preplan to support critical assets within their service footprints.

The third circle includes the still larger array of defense installations, including National Guard bases, which would be essential for providing defense support to civil authorities if disruptions of the grid jeopardize public health and safety.<sup>168</sup> During Hurricane Maria (2017), Superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, lodging, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and delivering other assistance. Protecting or rapidly restoring the reliability of the defense critical electric infrastructure that supports

<sup>165</sup> See DOD, *Manual 3020.45*; and DOD, *Directive 3020.40*.

<sup>166</sup> DOD, *Directive 3020.40*.

<sup>167</sup> DOD, *Manual 3020.45*.

<sup>168</sup> Of course, many National Guard installations that could conduct defense support operations may also be responsible for assisting war fighting operations abroad, and would therefore fall within the second circle as well.



these defense-support-to-civil-authorities functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public.<sup>169</sup>

Building preparedness for grid security emergencies can also help meet an underlying challenge for deterrence: attack attribution. To convince foreign leaders that they will suffer swift and costly consequences if they strike the grid, those leaders must first believe that the United States will be able to identify them as the attackers.<sup>170</sup> The Federal Bureau of Investigation (FBI) and other federal agencies are improving their attribution capabilities.<sup>171</sup> US agencies also devote massive resources to human and technical intelligence collection on potential adversaries, which could further assist attack attribution.<sup>172</sup> Nevertheless, adversaries may seek to strike in ways that complicate attack forensics by employing wiper tools and using other tactics, techniques, and procedures to cover their tracks.<sup>173</sup>

Emergency orders can help defeat adversaries' efforts to evade attribution. By refining the FPA's information sharing mechanisms and building them into emergency orders, utilities and their government partners can strengthen their ability to share malware samples and other information on threat signatures.<sup>174</sup> New technologies can bolster such collaboration. For

example, the Containerized Application Security for Industrial Control Systems project is designed to help grid operators isolate and capture malware on their systems, enabling samples to be shared with government agencies while still preventing that malware from disrupting system operations.<sup>175</sup>

Developing emergency orders and implementation plans to defend the grid can also provide broader support for attribution. James Miller notes that "while cyber hardening of US critical infrastructure will never be good enough to prevent a Russia or China from being able to threaten a major attack, it can cause them to have to be 'noisier' to do so, thereby boosting our confidence in attribution."<sup>176</sup> Emergency measures to protect grid reliability can complicate attack planning and, ideally, drive adversaries to strike in ways that will make them easier to identify.

### **Deterrence by Denial: Protecting Critical Electric Infrastructure**

Convincing adversaries that they will suffer unacceptable costs if they strike the grid is only one means of deterring such attacks. Another means is to reduce the benefits that adversaries expect to achieve by attacking. In classical deterrence theory, both factors combine to influence an adversary's decision on whether to strike. As Joseph Nye Jr. puts it, "deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."<sup>177</sup>

The *National Security Strategy* calls for measures that can prevent attackers from achieving the goals they seek and thereby strengthen deterrence by denial. The strategy states that "we must ensure the ability to deter enemies by denial, convincing them that they cannot accomplish their objectives through the use of

<sup>169</sup> Countering such adversary efforts will also require protecting electric service to financial institutions, regional hospitals, and other civilian assets essential to the US economy and public health and safety. The next section of the report examines these requirements and their implications for deterrence and emergency order design.

<sup>170</sup> On the tasks that attribution comprises, see Lin, "Escalation Dynamics," 49–50.

<sup>171</sup> Smith, "Roles and Responsibilities." See also Newman, "Hacker Lexicon."

<sup>172</sup> Miller, "Cyber Deterrence."

<sup>173</sup> Newman, "Hacker Lexicon."

<sup>174</sup> See 16 U.S.C. § 824a–1, (d). Later sections of this report provide a more detailed assessment of provisions for improved information sharing.

<sup>175</sup> "Sandia's Grid Modernization Program Newsletter," Sandia National Laboratories.

<sup>176</sup> Miller, "Cyber Deterrence."

<sup>177</sup> Nye, "Deterrence and Dissuasion," 45.

force or other forms of aggression.”<sup>178</sup> Ensuring that the grid and other infrastructure sectors can survive attacks and rapidly recover from service interruptions plays an especially important role in the administration’s deterrence posture. The strategy notes that “a stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.”<sup>179</sup> More recent statements of administration policy also note that deterrence by denial “must be foundational to the U.S. deterrence approach,” and that US efforts must continue “to deny adversaries the benefits of their malicious cyber activities.”<sup>180</sup>

Emergency orders and implementation plans may be able reduce the benefits that adversaries expect to achieve by attacking the grid. Preattack orders to bolster grid defenses can impede adversary efforts to disrupt grid reliability. Once attacks are under way, orders for prioritized load shedding and other extraordinary measures can help limit the damage the adversaries may hope to inflict on financial institutions, hospitals, and other electricity-dependent facilities. Orders that accelerate power restoration to these critical facilities may also reduce the effects of an attack, and thereby strengthen deterrence by denial.

The FPA is ready-made to support such improvements. In addition to protecting defense critical electric infrastructure, and thereby assisting deterrence through cost imposition, the act also authorizes orders to protect a much broader portion of the grid: critical electric infrastructure. Such infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>181</sup> Orders to help utilities defend critical electric infrastructure can reinforce deterrence by denial—and, if deter-

rence fails, reduce the devastation that adversaries will create.

However, developing and implementing such orders will entail major challenges. Some deterrence theorists doubt whether deterrence by denial is practical in cyberspace, in part because offensive capabilities are so much stronger than cyber defenses. The conclusion of this report will examine those arguments and explore broader opportunities to bolster deterrence and help the United States defeat our adversaries if conflicts nevertheless occur. First, however, DOE and its partners will need to overcome two impediments to protecting critical electric infrastructure: determining which specific facilities and functions are truly critical, and securely sharing that information with utilities so they can refine their operational plans for grid security emergencies.

### **Building a “Section 9+ List:” Prioritizing Infrastructure for Sustainment and Restoration**

Identifying and prioritizing critical electric infrastructure will be far more difficult than doing so for defense critical electric infrastructure. If adversaries create cascading blackouts across one or more interconnections, the disruption of many thousands of civilian-owned facilities could negatively affect national security, the US economy, and public health and safety. Utilities cannot possibly prioritize the flow of power to all such facilities. Government agencies and their private sector partners will need to determine which specific customers (and the critical electric infrastructure that serves them) are most vital to the nation and must continue to receive power if widespread instabilities occur.

Executive Order 13636 (February 2013) provides an existing methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the secretary of homeland security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security,

<sup>178</sup> White House, *National Security Strategy*, 28.

<sup>179</sup> White House, *National Security Strategy*, 13.

<sup>180</sup> DOS, *Recommendations*, 2.

<sup>181</sup> 16 U.S.C. § 824o–1, (a)(2).

or national security.”<sup>182</sup> That standard—catastrophic damage—provides a useful criterion to identify the highest-priority assets and associated critical electric infrastructure for protection by emergency orders in grid security emergencies. Over time, orders and contingency plans could gradually encompass less-critical facilities and grid infrastructure.

Of course, the section 9 methodology and subsequent list were never intended to support the implementation of section 215A of the FPA. As a result, the section 9 methodology falls short of meeting all the requirements for supporting emergency order design. One gap lies in the threats that drive the selection of critical assets. Section 9 focuses exclusively on infrastructure at risk from cyber attacks. The FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on electric systems. Executive Order 13636’s section 9 requirements also create a “corporate”-level list that is not broken down into the key assets within those corporations (i.e., facilities, systems, and nodes). More fine-grained data and analysis will be required to identify facilities for which sustained electric service will be most crucial. Efforts to prioritize grid service will also need to account for the increasingly complex interdependencies between US infrastructure sectors.<sup>183</sup>

Despite these shortfalls, Executive Order 13636’s methodology can provide a valuable starting point for identifying the most vital critical electric infrastructure and supporting assets. DOE and its industry partners should leverage that methodology to create a “section 9+” list, tailored to fulfill FPA emergency order requirements. Other government initiatives to prioritize critical infrastructure could

also make valuable contributions to the list and overall prioritization effort. For example, DHS’s May 2018 cyber strategy emphasizes the importance of “identifying the most critical [federal] systems and prioritizing protections around those systems.”<sup>184</sup> A number of other initiatives could provide significant value as well.<sup>185</sup> Building a section 9+ list would also benefit from the inclusion of input from cleared state regulators and homeland security and emergency management officials.

DHS’s National Risk Management Center can help integrate these sources of data and develop a comprehensive, cross-sector basis for prioritizing the sustainment and restoration of power to critical facilities. Government agencies within the center will collaborate with the private sector to “identify, assess, and prioritize efforts to reduce risks to national critical functions, which enable national and economic security.” One immediate task will be to “help define what is truly critical.”<sup>186</sup> As this work

<sup>184</sup> DHS, *Cybersecurity Strategy*, 8.

<sup>185</sup> There are numerous programs that DOE and its partners could leverage to build the section 9+ list. DHS’s National Critical Infrastructure Prioritization Program aims to identify “nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance.” See DHS, *NIPP 2013*, 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on “lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity” (p. 24). Despite its focus on terrorist threats, *Homeland Security Presidential Directive 7* also requires the secretary of homeland security to identify and prioritize systems and assets that, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the “loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States” and lower jurisdictions. The national-level priorities on this list could also be helpful. 6 U.S.C. § 124l, (a)(2).

<sup>186</sup> “National Risk Management Center Fact Sheet,” DHS.

<sup>182</sup> Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*.

<sup>183</sup> For methodologies and data-gathering strategies to assess cross-sector interdependencies, see EIS Council, *E-PRO Handbook III*; and Homeland Security Advisory Council, *Final Report*.

goes forward, the center's efforts could contribute to the development of a section 9+ list that will be essential for grid security emergency preparedness.

### **Sharing the Section 9+ List and Protecting Critical Electric Infrastructure Information**

In addition to identifying assets most in need of power, it will also be essential to share that data with the utilities responsible for providing prioritized service. Current section 9 guidance lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the federal government tells grid owners and operators if they are on the section 9 list, it rarely informs them about the section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own system configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data with government partners. Public sector leaders will need to reinforce their industry counterparts' confidence that government agencies will not use company-provided information for regulatory compliance, antitrust, or other purposes not explicitly approved through industry-government dialogue.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that critical companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations or supply chains in one industry can produce unintended and unforeseen effects on overall system resilience. Private

companies will need to help government agencies modify the section 9+ list as they reconfigure their operations and create new dependencies on outside service and product providers.

Securing and limiting the distribution of this classified data will also be a prerequisite for countering potential attacks. If adversaries acquired the section 9+ list, it would provide a roadmap that they could use to maximize their devastation of US critical infrastructure. However, measures to protect this data must be complemented by improved mechanisms to provide sensitive information to industry personnel who have the requisite security clearances.

Section 215A of the FPA offers a starting point to meet these requirements. The FPA provides for the sharing of critical electric infrastructure information, defined as information generated by FERC or other federal agencies related to identified (or proposed) critical electric infrastructure "that is designated as critical electric infrastructure information by the Commission or the Secretary" or that qualifies under FERC's critical energy infrastructure information scheme.<sup>187</sup> The FAST Act amendments directed FERC to facilitate the voluntary sharing of such information "with, between, and by" BPS entities and their government partners.<sup>188</sup> The amendments also require FERC to create criteria and procedures to designate certain information as critical and prohibit unauthorized disclosure of that information.<sup>189</sup> To help meet these requirements, FERC incorporated and is building on its well-established mechanisms to protect critical energy infrastructure information.<sup>190</sup>

<sup>187</sup> The definition excludes classified national security information. 16 U.S.C. § 824o-1, (a)(3).

<sup>188</sup> This includes NERC, the E-ISAC, regional entities, and "other entities determined appropriate by the Commission." See 16 U.S.C. § 824o-1, (d)(2)(D).

<sup>189</sup> 16 U.S.C. § 824o-1, (d)(2).

<sup>190</sup> FERC, *Regulations Implementing FAST Act Section 61003* (Order No. 833), 157 FERC ¶ 61,123, 13. See also FERC,



Other initiatives are also under way to provide for the protected data sharing essential for preplanning grid security emergency operations. DOE is working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate assets identified as defense critical electric infrastructure. Going forward, DOE, FERC, and their industry partners should refine their equivalent mechanisms to securely distribute data on critical electric infrastructure and the water systems, communications centers, and other essential non-defense assets that must continue to function in grid security emergencies.

## Communications Requirements for Issuing and Employing Emergency Orders

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phones and other normal means of communication fail. These systems often provide connectivity with neighboring BPS entities and, to an increasing extent, entities that are farther away. Under the ESCC, industry has also built an extensive set of playbooks to help companies decide what to tell customers about an incident and to unify messaging between government officials and industry representatives on estimated times of restoration and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. Preparedness for grid security emergencies will require additional progress in four areas: (1) refining consultative mechanisms and protocols for the sequential (though potentially overlapping) phases of such emergencies; (2) ensuring that communications

systems can survive adversaries' attacks; (3) authenticating emergency orders and protecting the security of sensitive data; and (4) determining what to say to the US public and accounting for the risk that adversaries will conduct information warfare operations to intensify panic and incite disorder.

## Initial Consultations and Sustained Communications

As with the phases of grid security emergency declarations, the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Preattack consultations constitute the initial stage. As noted above, the FPA specifies that before the secretary issues emergency orders, DOE will consult with power companies and other BPS stakeholders "to the extent practicable . . . regarding implementation of such emergency measures."<sup>191</sup> This report recommends that federal officials also consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The grid security emergency rule clarifies how DOE's Office of Electricity Delivery and Energy Reliability will consult on emergency orders.<sup>192</sup> The rule states that, if practicable, the E-ISAC is one of the organizations the secretary will consult. Such consultations will be particularly useful for sharing data (including classified data) on attacks that are imminent or under way. The rule also notes that DOE will consult with the ESCC. The ESCC will provide an especially valuable source of industry perspectives on grid security emergency declarations and emergency orders because it represents all components of the electricity subsector and has extensive experience in coordinating the industry's incident response operations. In addition, the rule states that "efforts

*Regulations Implementing FAST Act Section 61003* (Order No. 833-A), 163 FERC ¶ 61,125; and 18 CFR 388.113.

<sup>191</sup> DOE, "RIN 1901-AB40," 1774.

<sup>192</sup> DOE, "RIN 1901-AB40," 1181.



will be made” to consult with NERC, regional entities, “owners, users, or operators” of critical and defense critical electric infrastructure (including regional transmission operators), appropriate federal and state agencies, and other grid reliability stakeholders.

Issuing emergency orders constitutes the second stage. DOE’s grid security emergency rule states that the department will “communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances.”<sup>193</sup> The E-ISAC will likely play a critical role in such communications, since it maintains a detailed, continuously updated list of all BPS owners, operators, and registered users (distribution entities). DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.<sup>194</sup> As long as these mechanisms can be hardened as necessary to survive adversaries’ attacks, leveraging them for grid security emergencies will be much more efficient than creating a separate, unfamiliar system for communicating emergency orders.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders. Attacks on the grid are unlikely to be “one and done.” As adversaries continue to try to destabilize the grid, and power companies respond with emergency operations to protect and restore electric system reliability, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional orders and response activities—potentially on a nationwide basis.

Reliability coordinators will be a critical touchpoint between DOE and individual BPS entities, serving as a focal point between DOE (and other government

leaders) and the power companies that are in their purview. This positioning makes them well suited to communicate secretary-issued orders to individual utilities. Moreover, given reliability coordinators’ responsibilities and authorities to help maintain grid reliability when incidents occur, they will also be ideally positioned to understand how grid security emergency orders should supplement BPS emergency operations that are already under way.

Sustained communications will also be necessary to meet an additional FPA requirement: responding to DOE requests for information on the implementation of emergency orders. The grid security emergency rule specifies that “beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order.”<sup>195</sup> Sustained communications links between DOE and BPS entities will be required to meet such requests for information. However, beyond compliance issues, continuous communications will also be required as government and industry partners assess the effectiveness of emergency operations and identify requirements for additional actions.

### Survivability of Communications

Adversaries will have compelling incentives to combine attacks on the grid with strikes against US communications systems. The 2015 attack on Ukraine’s electric grid illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone networks; the latter attack prevented customers from reporting outages and disrupted grid operators’ ability to conduct restoration operations.<sup>196</sup> In turn, if adversaries can lengthen power outages by disrupting communications systems essential

<sup>193</sup> DOE, “RIN 1901-AB40,” 1181.

<sup>194</sup> DOE, “RIN 1901-AB40,” 1177.

<sup>195</sup> DOE, “RIN 1901-AB40,” 1182.

<sup>196</sup> “Alert (IR-ALERT-H-16-056-01).”

for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications-system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually reinforcing disruptions in both sectors.

We should assume that adversaries will design their attacks to maximize multisector failures, especially since they would already be facing the risk of US response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry–government coordination in grid security emergencies. Enemies might strike communications systems to hobble efforts to share preattack threat data and convey emergency orders. Once attacks on the grid were under way, adversaries could also seek to cripple the communications systems needed to coordinate emergency operations and assess requirements for additional measures.

Strengthening the survivability of existing communications links will be essential to manage these risks. To date, ESCC consultation and coordination mechanisms have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to distributed denial-of-service attacks and a range of other increasingly severe threats,<sup>197</sup> as well to the loss of the grid-provided electricity on which many such systems depend (especially in long-duration outages that put emergency power assets at risk).

Adversaries may also seek to disrupt systems essential for information sharing. For example, the Cybersecurity Risk Information Sharing Program and other E-ISAC notification procedures and portals are in place to alert utilities when adversaries

are implanting malware on critical systems.<sup>198</sup> This includes the E-ISAC’s new Critical Broadcast Program, which is intended to operationalize the organization’s information sharing capabilities.<sup>199</sup> The FBI and DHS also issue alerts to the energy sector, as in the case of CrashOverride.<sup>200</sup> However, many of these warning and information sharing mechanisms rely on the internet or other potentially vulnerable systems. Industry and government should explore options to ensure that they can still convey essential data in the face of sophisticated attacks on the communications sector.

In addition, adversaries may seek to disrupt the issuance of emergency orders. DOE’s grid security emergency rule notes that the department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include “essential actions” to protect BPS reliability, which require recipients to respond as defined in the alert.<sup>201</sup> DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across registered entities. NERC already distributes alerts broadly to BPS users, owners, and operators in North America. Hence, the alert system provides DOE with an opportunity for “one-stop shopping” when issuing emergency orders. The secretary could issue an order to NERC for distribution to both regional operating organizations (regional transmission organizations, independent

<sup>197</sup> Banham, “DDoS Attacks.”

<sup>198</sup> “Energy Sector Cybersecurity Preparedness,” DOE; and “Electricity Information Sharing and Analysis Center,” NERC.

<sup>199</sup> The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See Lawrence, de Seibert, and Daigle, “E-ISAC Update.”

<sup>200</sup> “Alert (TA17-163A).”

<sup>201</sup> “About Alerts,” NERC.

system operators, reliability coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is email based.<sup>202</sup> As such, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also includes only those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for implementing emergency orders for prioritized load shedding and other actions to sustain power to critical facilities.

Moreover, while the NERC alert system could provide a means of communications across BPS users, owners, and operators, NERC primarily uses the system to communicate alerts of voluntary actions to be taken by electric industry stakeholders. Using the NERC alert system to instead communicate a mandatory action pursuant to a DOE emergency order would require clear coordination and communication to ensure that the order and associated requirements for action are fully understood. In addition, while the NERC alert system offers a proven means to convey unclassified information, the system may not be well suited to distribute classified data.

To fill these gaps, industry and government partners should consider measures to bolster the NERC alert system or create fallback options for survivable communications. Satellite phones offer a prominent option for operational coordination. These phones are widely deployed both among BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies.

Retired US Air Force General William Shelton, who directed the US Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community."<sup>203</sup>

Accordingly, power companies are ramping up their investments in terrestrial emergency communications systems that are hardened against cyber and physical attacks and can be used to sustain critical grid functions even if satellite phones fail.<sup>204</sup> Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are under way to build dark fiber or other survivable links between BPS entities—much less between those entities and DOE. The National Infrastructure Advisory Council study *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish "separate, secure communications networks specifically designated for the most critical cyber networks, including 'dark fiber' networks for critical control system traffic and reserved spectrum for backup communications during emergencies."<sup>205</sup>

The council's study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. In doing so, DOE should leverage lessons learned from the communications sector and specifically from the National

<sup>202</sup> "About Alerts," NERC.

<sup>203</sup> Shelton, "Threats to Space Assets," 3.

<sup>204</sup> FERC and NERC, *PRASE*, 15.

<sup>205</sup> NIAC, *Securing Cyber Assets*, 7.

Security Telecommunications Advisory Committee, which has extensive experience in building redundant and survivable systems.<sup>206</sup> However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities “can communicate with utility crews working in the field to manually restore power” and conduct other postattack operations.<sup>207</sup> Survivable communications systems must also be able to coordinate emergency operations across the electricity subsector and with supporting government agencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when those orders are needed most.

### Authenticating and Securing Emergency Orders

In addition to disrupting the availability of communications systems, adversaries may also seek to corrupt the content of emergency orders and coordination messages, and gain access to classified US data to help defeat grid protection measures. One near-term requirement will be to ensure that utilities can authenticate the orders they receive from DOE. Power companies will need to be able to verify that an order has actually come from the secretary, and that adversaries have not altered its content. Verifying the authenticity of orders will be especially important if such orders require extraordinary measures that could further disrupt normal service and affect public health and safety.

Existing mechanisms and protocols to ensure the integrity of subsector communications provide an initial basis to meet these challenges. Other government agencies have also developed authentication protocols that could be adapted for use in grid security emergencies. For example, the *DoD Cybersecurity Discipline Implementation Plan* (February 2016) offers detailed guidance to strengthen authentication in the face of adversary

efforts to exploit communications networks and devices.<sup>208</sup>

Adversaries may also seek to gain access to classified or operationally sensitive emergency orders. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as possible, lest those operations create incentives for adversaries to strike before their advanced persistent threats were disabled. When attacks are under way, it could be useful to deny adversaries the knowledge of where and how BPS entities are prioritizing the flow of power to vital military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important, given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The FPA and subsequent grid security emergency rule provide for the sharing of classified information in grid security emergencies. The rule specifies that:

To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.<sup>209</sup>

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program already have mechanisms and protocols for sharing and securing classified threat

<sup>206</sup> “About NSTAC,” DHS.

<sup>207</sup> NIAC, *Securing Cyber Assets*, 7.

<sup>208</sup> DOD, *DoD Cybersecurity Discipline Implementation Plan*.

<sup>209</sup> DOE, “RIN 1901–AB40,” 1182.



data with BPS entities cleared for access to that data.<sup>210</sup> Industry and government partners should consider building on those mechanisms to support the issuance of classified emergency orders. Ongoing progress under the Cybersecurity Risk Information Sharing Program will be valuable as it serves a growing array of utilities, accesses additional sources of data and advanced analytic tools, and continues other improvements.

DOE and its partners in industry and government might consider sharing this classified data in other ways. For example, DHS and other federal partners such as the FBI and the National Guard have secure video teleconference capabilities. However, these are technologically complex and not seamlessly interoperable with industry systems. Moreover, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Section 215A addresses this issue by ordering the secretary to “facilitate and, to the extent practicable, expedite,” the security clearance process for key personnel of any entity subject to emergency orders to enable “optimum communication” of threat information.<sup>211</sup> DOE should accelerate its ongoing efforts to meet this requirement. The section also grants the secretary and other appropriate federal agencies the authority to provide temporary access to classified information regarding grid security emergencies and subsequent orders to key personnel of complying entities.<sup>212</sup>

Yet, even for utilities with cleared personnel on their staffs, an even smaller number possess the sensitive compartmented information facilities or other infrastructure and government approvals to store classified information. To address those limitations, the grid security emergency rule clarifies that the secretary may declassify information critical to the

emergency response.<sup>213</sup> But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of combatant commander operational plans; when emergency orders may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

### Communicating with the American People

Adversaries may attack the grid not only to disrupt national defense and the economy but also to gain political leverage over US leaders by inciting public panic and disorder. A presidential declaration that the grid faces imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the US public.

Preplanning for public messaging to accompany grid security emergency declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Unifying messaging with governors and other elected officials on estimated restoration times already presents significant challenges in such events. However, those difficulties will be dwarfed by the problems that adversaries can create through cyber attacks. Attackers may:

- Use information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety
- Intensify state and local requests for defense support to civil authorities to deal with these

<sup>210</sup> “Energy Sector Cybersecurity Preparedness,” DOE.

<sup>211</sup> 16 U.S.C. § 824o–1, (e).

<sup>212</sup> 16 U.S.C. § 824o–1, (b)(7).

<sup>213</sup> DOE, “RIN 1901–AB40,” 1778.



anticipated effects, and thereby put pressure on US leaders to divert scarce defense assets and resources from other missions

- Disrupt normal means of communication on which the public will rely for information about the event
- Magnify the inherent difficulties of estimating restoration times by employing advanced persistent threats that enable repeated reattacks and disruptions in grid service until eradicated from BPS networks.

DHS's Social Media Working Group for Emergency Services and Disaster Management has offered preliminary recommendations on how to counter disinformation during disaster response operations.<sup>214</sup> In addition, the ESCC and its members are developing playbooks to help meet disinformation challenges and support public messaging in the event of cyber or physical attacks against the grid.<sup>215</sup> Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that presidential grid security emergency declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Preplanning for message coordination with Canada and Mexico could also be helpful and might leverage the FPA's provisions for such multinational consultations concerning the issuance of emergency orders.<sup>216</sup>

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. For example, some orders that will be valuable for protecting grid reliability, including those for prioritized load shedding, could

cut off electricity to many thousands of customers to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

## The Deeper Value Proposition for Emergency Orders: Political Top Cover, Waivers, and Cost Recovery

The grid security emergency provisions of the FPA do not even mention a significant advantage that orders can provide for industry: they can help protect power companies from the political heat that extraordinary grid protection measures will create. The FPA's provisions for regulatory waivers and cost recovery offer more explicit benefits. Yet, given the risks that utilities could incur in conducting emergency operations, and the investments in infrastructure that may be required to facilitate order implementation, Congress and DOE should consider additional measures to help power companies defend the grid and protect national security.

### Facilitating Operations under Extraordinary Political Circumstances

In responding to natural hazards, power companies can fall under intense pressure to serve the priorities of state and local elected officials. In severe weather events, for example, governors have told utilities to delay sending restoration resources to assist neighboring states until service has been restored to *all* customers (i.e., voters) in the governors' own states.

Cyber and physical attacks on the grid could create still more intense political pressure, and complicate utilities' efforts to serve national priorities versus those most urgent to meet state and local needs. Such attacks will occur in the context of broader risks of all-out war and will magnify public fears in ways that hurricanes or other natural hazards cannot—especially if those attacks are accompanied by

<sup>214</sup> Social Media Working Group for Emergency Services and Disaster Management, *Countering False Information*.

<sup>215</sup> ESCC, "ESCC: Electricity Subsector Coordinating Council."

<sup>216</sup> 16 U.S.C. § 824o-1, (b)(3).

information warfare operations to incite public panic. Governors will have powerful incentives to ensure that utilities in their states take care of their own citizens rather than meeting requests for assistance from power companies in other states.

However, from a national security perspective, not all states and customers within them will be of equal importance for protecting defense critical electric infrastructure. Some low-population states served by utilities with only limited resources are the homes of vital military installations. These utilities may need assistance from out-of-state power companies to supplement their own personnel and response capabilities when adversaries strike.

The electric industry's Cyber Mutual Assistance (CMA) Program will be critical for providing such support.<sup>217</sup> DOE is expanding the technical resources and capabilities available to support CMA response operations.<sup>218</sup> Under the national response event initiative, investor-owned utilities (led by the Edison Electric Institute) are also bolstering mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States.<sup>219</sup> All of these initiatives will be vital for responding to grid security emergencies that entail multiregional disruptions of the BPS or degrade critical electric infrastructure that the infrastructure's owners cannot restore on their own.

Yet, the voluntary nature of these mutual assistance systems could present challenges in grid security emergencies. In hurricanes or other natural hazards, governors and utilities can predict whether or not their states are likely to be struck and either husband their resources accordingly or provide them in response to requests for assistance. Cyber and physical attacks by Russia, China, or other potential adversaries are much less predictable. Enemies may

strike one region before moving on to others. Attacks could even occur on a nationwide basis. Accordingly, elected officials may discourage utility leaders from volunteering resources for mutual assistance in neighboring regions, even if their own states have not yet been struck.

Issuing emergency orders can help utilities address these challenges and serve national priorities. Participants in the Cyber Mutual Assistance Program are already taking steps to account for the risk of multiregional attacks. DOE and its industry partners should preplan to reinforce those measures in grid security emergencies. If the secretary orders utilities to help protect or restore grid reliability beyond their service areas, those orders will help justify (and indeed, legally require) providing such assistance, regardless of the political pressure against doing so. DOE should consider reaching out to state and local leaders and their senior energy appointees before emergencies occur in order to ensure that they are familiar with the FPA requirements and the national security value of mutual assistance.

Emergency orders can also help utilities execute politically unpopular emergency operational decisions within their own service areas. Cyber and physical attacks could put utility CEOs in the unenviable position of having to manage shortfalls in available power by depriving lower-priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The secretary of energy can give CEOs political top cover for taking such unpopular actions, rather than leave them to act on a voluntary basis and bear the full brunt of explaining why they did so.

Exercises can help utilities and government officials prepare to collaborate in the face of intense political pressures, and coordinate the execution of emergency orders on a nationwide basis. NERC already requires BPS entities to exercise their individual emergency and power system restoration plans. In the GridEx exercise series, over one hundred utilities across the

<sup>217</sup> ESCC, "Cyber Mutual Assistance Program."

<sup>218</sup> DOE, *Multiyear Plan*, 29.

<sup>219</sup> EEI, *Understanding the Electric Power Industry's Response and Restoration Process*.

United States and Canada test the use of their plans against combined cyber-physical attacks and exercise the use of Cyber Mutual Assistance protocols and procedures. Building template emergency orders and utility-specific implementation plans will provide an even stronger basis for coordinated multientity exercises. In planning for GridEx V in 2019, NERC and its government and industry partners should consider the possibility of exercising the issuance and implementation of specific template emergency orders. State, local, tribal, and territorial participation in utility exercises that include the use of emergency orders will also be crucial.

### Environmental, Regulatory, and Legal Waivers

In amending the FPA to address grid security emergencies, Congress provided power companies with an important protection for complying with emergency orders—one that they might not receive by implementing equivalent emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate FERC-approved grid reliability standards or other rules or provisions under the FPA, the act specifies that those actions “shall not be considered a violation” of those provisions. Such waivers of enforcement apply unless a complying entity acts in a “grossly negligent manner.”<sup>220</sup>

The FAST Act amendments to the FPA also introduced broader protections into section 202(c), absolving entities from violations of federal, state, or local environmental laws or regulations that occur as a result of complying with an order. That provision shields complying entities from “any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation.”<sup>221</sup> These protections apply to section 215A emergency orders as well.<sup>222</sup>

FPA-based waivers will be especially valuable for certain types of emergency orders. For example, if the secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service, such as proactively shedding firm load, could also violate NERC’s FERC-approved reliability standards.<sup>223</sup> Separating preplanned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards as well.

The waiver process under the FPA is structured to function automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that a BPS entity has acted with gross negligence. Nevertheless, industry, DOE, and regulators might find it useful to build consensus on the types of waivers that specific template orders should include.

Their discussions could also help address more far-reaching regulatory issues that grid security emergencies may pose. For example, the FPA does not provide waivers for Nuclear Regulatory Commission regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the commission would enforce a violation of its regulations by a nuclear generation entity complying with an emergency order. The worst time to adjudicate such a dispute, however, would be in the midst of a grid security emergency. Pre-event discussions will be particularly important given the nuclear fleet’s imperative to protect public health and safety. DOE, the Nuclear Regulatory Commission, and their industry partners will need to ensure that assessments of regulatory issues associated with

<sup>220</sup> 16 U.S.C. § 824o–1, (f)(4).

<sup>221</sup> 16 U.S.C. § 824a, (c)(3).

<sup>222</sup> 16 U.S.C. § 824o–1, (f)(2).

<sup>223</sup> For example, in events such as the September 2011 Arizona–California disturbance, FERC has found that load shedding led to violations of NERC’s reliability standards.

emergency operations take safety considerations into full account.

Preplanning will also be vital for emergency orders that support power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that “the storage of strategically located spare large power transformers” and other critical grid components “will reduce the vulnerability of the United States to multiple risks facing electric grid reliability,” including cyber and physical attacks.<sup>224</sup> Accordingly, Congress required DOE to develop a strategic transformer reserve plan to determine the number and type of spare large power transformers that should be stored and to examine issues associated with transporting those spares.<sup>225</sup>

DOE responded to this requirement by providing a strategic transformer reserve report (March 2017). The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a more substantial pool of spare large power transformers than DOE had anticipated and that a federally owned reserve is not needed.<sup>226</sup> However, the plan also found that it was crucial to ensure that large power transformers can be efficiently moved during national emergencies.<sup>227</sup>

Regulatory waivers can play a critical role in facilitating that movement. The higher-voltage classes of large power transformers, including 765-kilovolt transformers, are as big as a house and can be moved—slowly and very carefully—only by specialized heavy-haul trucks, railcars, and barges. Under the auspices of the ESCC, utilities have established the Transformer Transportation Working Group to analyze the problems posed by moving large power transformers in an emergency

and to build collaborative plans with transportation companies and associations. A central finding of the group’s analysis: regulatory waivers will be critical to expedite the movement of large power transformers, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.<sup>228</sup>

DOE’s 2017 transformer report committed the department to coordinating with the Transformer Transportation Working Group “to improve and optimize transportation planning in response to a significant national event impacting the electricity grid.”<sup>229</sup> However, the report did not examine how emergency orders and implementation plans might speed the transportation of large power transformers. As DOE collaborates with the working group and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols that are not addressed by the FPA and that pose the greatest impediments to transformer movement. DOE and its partners should then preplan to waive these provisions if the secretary issues emergency orders.

The challenge for such preplanning: the secretary of energy lacks the statutory authority to waive key transportation regulations. Most federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of DOT. Federal regulations and emergency operations that would govern the movement of transformers on barges, which could be critical for restoring power for coastal cities and along the Mississippi–Ohio river system of inland waterways, are overseen by the US Coast Guard and the US Army Corps of Engineers. State and local transportation regulations and permitting requirements will also

<sup>224</sup> FAST Act, 1779.

<sup>225</sup> FAST Act, 1780–1782.

<sup>226</sup> DOE, *Strategic Transformer Reserve*, 21.

<sup>227</sup> DOE, *Strategic Transformer Reserve*, 1.

<sup>228</sup> ICF, *Assessment of Large Power Transformer Risk Mitigation Strategies*, 22–23.

<sup>229</sup> DOE, *Strategic Transformer Reserve*, 22.



pose major impediments to moving large power transformers over roads unless adequate waivers are in place to lift restrictions.

DOE should build collaborative plans to employ waiver authorities beyond those directly under the secretary's control. For example, to facilitate the movement of large power transformers, gubernatorial disaster declarations could help waive state-level regulations. The American Association of State Highway and Transportation Officials and National Emergency Management Association are exploring the use of these and other waiver authorities. DOE is also preplanning with other federal, state, local, tribal, and territorial agencies to coordinate response operations under Emergency Support Function #12—Energy.<sup>230</sup> Especially valuable, a growing number of individual power companies are creating contingency plans for emergency transportation with government agencies and road, rail, and barge companies. Building on these efforts, and on initiatives led by the Transformer Transportation Working Group,<sup>231</sup> the electricity subsector and its partners should establish systematic, nationwide plans to facilitate the movement of transformers and other critical equipment in grid security emergencies.

Over the longer term, Congress, industry, and government partners should also consider whether complying entities should have liability protections beyond those currently provided by the FPA. Prioritized load shedding for extended periods will create “winners and losers” in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other section 9+ assets may leave shortfalls in electric service at dialysis centers, small urgent-care centers, and facilities for special-needs citizens. These disruptions will put lives at risk. Legislators, DOE, and electric industry leaders should examine whether utilities complying

with such necessary but highly disruptive emergency orders ought to have additional liability protections. Cutting off power to lower-priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.<sup>232</sup> Again, if these risks of exposure are sufficiently severe, Congress should consider providing further protections for BPS entities.

### **Cost Recovery for Emergency Operations and Support for Investments in Grid Infrastructure**

Complying with emergency orders may force utilities to incur costs beyond their normal operating expenses. The FPA states that if FERC determines “that owners, operators, or users of critical electric infrastructure have incurred substantial costs” in complying with an emergency order, FERC shall “establish a mechanism that permits such owners, operators, or users to recover such costs.”<sup>233</sup> Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other orders could require reimbursement through FERC-directed mechanisms as well.

The act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that emergency orders require utilities responsible for defense critical electric infrastructure to take emergency measures, the “owners or operators” of critical defense facilities that rely on such infrastructure “shall bear the full incremental costs of the measures.”<sup>234</sup> Fair warning to DOD: it

<sup>230</sup> “State and Local Energy Assurance Planning.” DOE.

<sup>231</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>232</sup> Frankel, “Can Customers Sue Power Companies for Outages?”

<sup>233</sup> The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs “prudently” and that those costs “cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users.” 16 U.S.C. § 824o–1, (b)(6)(A).

<sup>234</sup> 16 U.S.C. § 824o–1, (b)(6)(B).



should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- attacks create major blackouts and deprive utilities of revenue;
- emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- adversaries disrupt financial markets, either through direct cyber attacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.<sup>235</sup>

Power companies are strengthening their plans and capabilities for cross-sector support with the financial services sector.<sup>236</sup> These efforts should include the development of contingency plans for financial-services companies (in coordination with the Department of Treasury and DOE) to help utilities cover the urgent expenses they may incur in responding to grid security emergencies. In addition, to facilitate the reimbursement process provided for in the FPA, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with orders will be more difficult once attacks are under way.

Cost recovery for investments in grid infrastructure to facilitate emergency order implementation will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. Other orders may be impossible to execute unless BPS entities make additional investments in infrastructure. It will be near useless to order transmission operators to protect or rapidly restore service to vital but remote military bases served by a single transmission line if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure that these facilities can help defeat US adversaries when the nation is under attack. DOD will need to develop a cost-recovery mechanism to reimburse defense critical electric infrastructure owners for making such investments.

To be even remotely viable as an emergency order design option, most preplanned power islands will also require at least some infrastructure construction. Ideally, these preplanned islands will use existing generation, transmission, and distribution assets within their service footprints to separate from the grid and still be able to provide reliable electric service to the section 9+ assets inside their borders. But many areas that might be designed to function as islands in a grid security emergency will lack adequate infrastructure to do so. The grid's interconnected design enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Preplanned power islands will not only lose those reliability benefits, but they will also have to make do with infrastructure that utilities built and aligned to be supporting components of the interconnected grid—not self-sustaining islands that would be stood up in grid security emergencies. Moreover, operating and recovering from preplanned island schemes will create an entirely different operating mode than industry is currently designed

<sup>235</sup> NERC, *GridEx III Report*, 15.

<sup>236</sup> See, for example, the Strategic Infrastructure Coordinating Council (SICC). ESICC, "ESICC: Electricity Subsector Coordinating Council."

for. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: to be effectively implemented, many emergency orders could require spending on new transmission lines and other grid infrastructure.

The FPA provisions for grid security emergencies do not explicitly authorize reimbursement for infrastructure investments. While the act requires FERC to establish a mechanism to enable owners, users, and operators of critical and defense critical electric infrastructure to recover their costs of complying with emergency orders, those funding provisions do not mention preattack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover costs for infrastructure investments in resilience against cyber and physical attacks.<sup>237</sup> FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate emergency order execution.

Similar discussions will be necessary with state public utility commissions. As noted above, local distribution systems will play vital roles in implementing emergency orders. Public utility commissions have primary regulatory authority over such distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. They could also make important contributions to reviewing proposed implementation plans for emergency orders that would be executed within their respective states, particularly when local distribution systems would be necessary to implement the orders.

<sup>237</sup> See, for example, FERC, *Extraordinary Expenditures* (96 FERC ¶ 61,299), 1; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), 10–11; and FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), 60.

The FPA opens the door to such discussions. The act states that FERC and the secretary of energy “shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions.”<sup>238</sup> Initiating these discussions with the National Association of Regulatory Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has extensively analyzed criteria for assessing the prudence of investments against cyber and physical attacks and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

## Conclusions and Recommendations for Broader Progress

Taken together, the options for industry–government collaboration examined in this report constitute a massive undertaking for which Congress appropriated zero funding to utilities. Developing a sequenced, prioritized strategy to explore these options will help make doing so a more manageable task.

Potential emergency orders will differ not only in terms of the phases of an attack in which they would be most useful, and in the degree to which they will disrupt normal electric service, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create—especially those that fall into the no-regrets category. Utilities frequently use conservative operations to help protect grid reliability in severe weather events. A growing number of companies are

<sup>238</sup> 16 U.S.C. § 824o–1, (d)(4).

already building on that foundation to draft equivalent conservative operations against cyber and physical threats. Emergency orders based on these initiatives constitute “low-hanging fruit”; creating such orders offers an immediate opportunity for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging emergency order initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are under way, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. Improving communications survivability and preplanning to counter disinformation campaigns will also be crucial for grid security emergency preparedness. So, too, will be efforts not only to fully leverage the FPA’s regulatory waiver and cost recovery mechanisms but also to explore additional liability protections and other measures to help entities comply with emergency orders.

A comprehensive plan to align and integrate these initiatives should also address three additional opportunities to build resilience for grid security emergencies: (1) preplanning to use additional federal and state emergency authorities to defend natural gas systems, communications networks, and other infrastructure on which the grid depends; (2) coordinating with Canada, Mexico, and other nations whose grids may be struck in conjunction with attacks on US electric systems; and (3) exploring new options to deter and defeat attacks on the grid by integrating defensive measures with government operations to blunt further strikes on US power companies and other targets.

## Employing Additional Emergency Authorities for Cross-Sector Resilience

Building preparedness against attacks on the grid is necessary but not sufficient to protect BPS reliability. In many US regions, power generation is becoming extraordinarily dependent on the flow of natural gas. Adversaries may attempt to cause cascading blackouts and other major grid instabilities by crippling natural gas systems. To hedge against such disruptions, some generators have the ability to operate on diesel and other secondary fuels if attackers interrupt gas supplies. But the refining and transportation systems needed to resupply such “dual-fuel” generators with diesel will themselves be at risk in grid security emergencies.<sup>239</sup> Moreover, as examined earlier in this report, coordinated grid restoration will also depend on the availability of communications systems and other infrastructure sectors.

This report has focused on employing the emergency authorities that Congress incorporated into the FPA by creating section 215A of the act in 2015. However, these authorities apply only to BPS owners and operators. The secretary cannot issue emergency orders under 215A to operators of natural gas and diesel fuel systems, much less to telecommunications companies and other infrastructure owners beyond the energy sector. The secretary has a range of other emergency authorities, including the Defense Production Act (DPA) and the authorities provided by section 202(c) of the FPA, which could facilitate coordinated response and restoration operations across the energy sector. The analysis that follows examines how DOE and its industry partners could preplan for the integrated use of all such authorities in a grid security emergency. This analysis also examines how federal and state leaders might use additional emergency powers to coordinate multisector response operations.

---

<sup>239</sup> The author has advised Exelon Corporation on risks of fuel interruptions for power generation. Exelon has provided no funding for this report.

## Coordinating Emergency Operations among Electric Utilities, Natural Gas Systems, and Other Energy Sector Components

Natural gas is an increasingly important source of fuel for power generation in many regions of the United States. Between 2002 and 2016, the nationwide share of electricity provided by gas-fired units increased from 18 percent to approximately 34 percent.<sup>240</sup> However, in New England, California, and other parts of the United States, natural gas has become the predominant source of fuel for power generation.

ISO New England has highlighted the risks that this reliance creates for grid resilience. It notes that “in New England, the most significant resilience challenge is fuel security—or the assurance that power plants will have or be able to obtain the fuel they need to run, particularly in winter—especially against the backdrop of coal, oil, and nuclear unit retirements, constrained fuel infrastructure, and the difficulty in permitting and operating dual-fuel generating capability.”<sup>241</sup>

Other regions also face growing fuel supply risks to grid resilience. A DOE-sponsored report titled *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units, Volume I: The Critical Role of Thermal Units During Extreme Weather Events* (March 2018) notes that many regional transmission organizations and independent system operators will face a combined challenge of inadequate natural gas pipeline infrastructure and competing demands for fuel from users apart from power generators.<sup>242</sup> More broadly, NERC has found that “the electric sector’s growing reliance on natural gas raises concerns regarding the ability to maintain BPS reliability when facing constraints on the natural

gas delivery systems.”<sup>243</sup> NERC’s 2016 *Long-Term Reliability Assessment* also notes that “as part of future transmission and resource planning studies, planning entities will need to more fully understand how impacts to the natural gas transportation system can impact electric reliability.”<sup>244</sup> Additionally, in *Grid Resilience in RTOs and ISOs* (January 2018), FERC called for additional data to better assess the risks posed by “wide-scale disruption to fuel supply” that could result in outages of multiple generators.<sup>245</sup>

Companies in the oil and natural gas subsector are bolstering their capabilities to protect their critical system components from attack and are taking new measures to ensure the continued safe and reliable delivery of natural gas to critical customers, including power generators.<sup>246</sup> However, threats to the oil and natural gas subsector are rapidly escalating as well.<sup>247</sup> As gas system owners and operators address these increasing threats, new opportunities will emerge for joint gas–electric resilience initiatives and emergency planning.

The oil and natural gas and electricity subsectors are already improving their coordination on resilience issues.<sup>248</sup> Moreover, NERC has been facilitating coordination between BPS entities and natural gas companies to address fuel resilience and interdependency challenges.<sup>249</sup> The ESCC has also been developing new coordination mechanisms for the

<sup>240</sup> DOE, *Staff Report to Secretary*, 90.

<sup>241</sup> ISO-NE, “Response of ISO New England Inc.,” 1.

<sup>242</sup> NETL, *Reliability, Resilience and the Oncoming Wave*, 4, 14, 22, 3.

<sup>243</sup> NERC, *Short-Term Special Assessment*, 12. See also NERC, *2013 Special Reliability Assessment*.

<sup>244</sup> NERC, *2016 Long-Term Reliability Assessment*, 21.

<sup>245</sup> FERC, *Grid Resilience*, 161 FERC ¶ 61,012 (2018), 14. See also Stockton, *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*.

<sup>246</sup> “Cybersecurity,” American Gas Association.

<sup>247</sup> Sobczak, Northey, and Behr, “Cyber Raises Threat”; and Stockton (on behalf of Exelon Corporation), *Prepared Direct Testimony* (Docket No. RM18-1-000), 13.

<sup>248</sup> DOE, *Staff Report to Secretary*, 94; and EIS Council, *E-PRO Handbook II*, 189.

<sup>249</sup> NERC, *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*, 1.



two industries (as well as with communications and financial services sectors).<sup>250</sup> Additionally, the natural gas industry participated in GridEx IV, which examined opportunities to mitigate the risk that adversaries will simultaneously attack gas and electric systems.

Building on these and other collaborative efforts, gas and electric companies (and their regulatory partners) should examine how they can prioritize support for each other in grid security emergencies. For example, when blackouts occur, electric companies typically prioritize the restoration of service to compression stations and other electricity-dependent gas infrastructure that is essential to supply fuel for power generation and other critical customers. Support for gas infrastructure should remain a priority, even as BPS entities add other section 9+ facilities to their restoration plans. Gas companies might also reassess their curtailment policies to help gas-dependent BPS entities sustain service to major military installations and other vital facilities in grid security emergencies.<sup>251</sup>

BPS entities and DOE should also pursue deeper collaboration with the companies that refine and deliver secondary fuels for power generation. If adversaries interrupt the flow of natural gas, dual-fuel generators can use diesel, no. 2 fuel oil, or other secondary fuels to sustain their operations in a grid security emergency.<sup>252</sup> However, cascading blackouts could disrupt the flow of these secondary fuels as well. Refining and transportation systems components that are essential to resupply dual-fuel generators depend on electricity. Adversaries may also attack these systems at the same time they strike the grid. Moreover, ongoing cutbacks in industry delivery capacity could magnify these risks of interruption. ISO New England notes that a “withering

delivery supply chain” constitutes an “unquantifiable X factor” in assessing grid resilience.<sup>253</sup> Preplanning to prioritize the delivery of secondary fuels for power generation will be essential for grid security emergencies, especially given the enormous demand for diesel from emergency power generators from hospitals, water utilities, and other vital facilities in wide-area blackouts.

Emergency authorities beyond 215A can help prioritize the flow of natural gas and secondary fuels to protect and restore grid reliability. The DPA will be especially helpful in this regard. The act is the “primary source of presidential authority to expedite and expand the supply of critical resources from the U.S. industrial base to support the national defense and homeland security.”<sup>254</sup> The DPA defines national defense to include “critical infrastructure protection and restoration,” encompassing all electric system components and supporting fuel supply infrastructure (including natural gas pipelines) that are at risk of cyber and physical attacks.<sup>255</sup> In 2012, the White House delegated many of the president’s DPA authorities to the heads of relevant federal agencies, including the secretary of energy for prioritization and allocation decisions regarding “all forms of energy.”<sup>256</sup>

Especially valuable for cross-sector resilience, DOE has established an Energy Priorities and Allocations System that enables the department to prioritize contracts for the delivery of natural gas, diesel, and other energy resources between the companies that provide them and government agencies, electric utilities, and other private and public sector customers. The system also enables DOE to allocate energy materials, services, and facilities to promote

<sup>250</sup> ESCC, “ESCC: Electricity Subsector Coordinating Council.”

<sup>251</sup> EIS Council, *E-PRO Handbook II*, 219.

<sup>252</sup> ISO-NE, *Operational Fuel-Security Analysis*, 52; and NERC, *2013 Special Reliability Assessment*, 4.

<sup>253</sup> ISO-NE, *Operational Fuel-Security Analysis*, 14, 16.

<sup>254</sup> DHS, *Power Outage Incident Annex*, 129.

<sup>255</sup> 50 U.S.C. § 4552, (14).

<sup>256</sup> Obama, *Executive Order—National Defense Resources Preparedness*.



“critical infrastructure protection and restoration” and emergency preparedness.<sup>257</sup>

DOE has already used its authorities under the DPA to support power generation in previous energy crises. In 2001, for example, the department used these authorities to ensure that emergency supplies of natural gas continued to flow to Californian power generators, thereby helping to avoid threatened electrical blackouts.<sup>258</sup> Now, to build preparedness for grid security emergencies, DOE and its industry partners should consider preplanning to use the DPA to sustain or restore gas and diesel deliveries to critical generators, including those that serve microgrids on defense installations, regional hospitals, and other assets critical for national security and public health and safety.

DOE could use the DPA to support and prioritize power restoration operations in other ways as well. Section 101(a) of the act provides DOE with the authority to prioritize the delivery of critical grid components in an emergency. If coordinated physical attacks damage or destroy transformers at a large number of critical substations, the secretary could use the DPA to allocate replacement transformers in ways that most directly benefit national security and public health and safety.

Two additional sources of emergency authorities could further strengthen preparedness and supplement the use of section 215A emergency orders. The first is section 202(c) of the FPA. The section authorizes the secretary to order “temporary connections of facilities and such generation, delivery, interchange, or transmission of electric energy as in its judgment will best meet the emergency and serve the public interest.” That provision also specifies that the secretary could exercise such powers “during the continuance of any war in which the United States is engaged, or whenever the Commission determines that an

emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy or of facilities for the generation or transmission of electric energy, or of fuel or water for generating facilities, or other causes.”<sup>259</sup>

A key virtue of section 202(c) is that the secretary can apply these emergency authorities to local distribution systems that might not fall within the purview of section 215A. Moreover, DOE has a strong record of having used 202(c) authorities in past emergencies, including the California Enron crisis, Hurricane Katrina, and other events.<sup>260</sup> DOE and its industry partners should consider building on this foundation to plan for the use of these authorities in grid security emergencies.

The Natural Gas Policy Act provides further authorities that could help coordinate energy sector operations in grid security emergencies. The president must declare a natural gas supply emergency before the secretary gains emergency powers under the act. The president can make such a declaration if there is evidence of an imminent or existing “severe natural gas shortage, endangering the supply of natural gas for high-priority uses” and that, having exhausted other alternatives “to the maximum extent practicable,” natural gas emergency authorities are necessary to resolve the situation.<sup>261</sup> The president may also delegate this authority, as well as the authority to issue rules or orders, to the secretary of energy or other appropriate federal officials.<sup>262</sup>

The president or secretary can issue two main types of orders or rules. Most important, during a natural gas supply emergency, the act authorizes the president or other officials to allocate natural gas supplies “to assist in meeting natural gas requirements for high-priority

<sup>257</sup> DOE, “RIN 1901-AB28,” 33615, 33622-33626.

<sup>258</sup> Brown and Else, *Defense Production Act of 1950*, 10.

<sup>259</sup> 16 U.S.C. § 824a, (c)(1).

<sup>260</sup> “DOE’s Use of Federal Power Act Emergency Authority,” DOE.

<sup>261</sup> 15 U.S.C. § 3361, (a).

<sup>262</sup> 15 U.S.C. § 3364, (d).

uses.”<sup>263</sup> The secretary could use this provision to ensure that critical generating facilities get the fuel they need.

Of course, some of these authorities overlap. DOE and its government and industry partners should develop an integrated approach to employing these powers for grid security emergencies, and determine which particular authorities are best suited to meet specific energy sector risks that cyber and physical attacks can create. These partners, along with other energy sector stakeholders, should also consider exercise scenarios that involve the simultaneous use of multiple emergency authorities to simulate the complex legal environment they may be faced with in a grid security emergency.

### **Multisector Resilience for Grid Security Emergencies**

An overarching strategy for grid security emergency preparedness should also advance operational coordination between energy companies and other infrastructure sectors that both rely on electricity and play vital roles in power restoration. Additional federal emergency authorities and incident response plans can help strengthen coordination between these interdependent sectors.

Using this broader array of plans and authorities will be particularly important if adversaries simultaneously attack multiple infrastructure sectors. By striking other sectors together with the grid, adversaries can exploit interdependencies between them to maximize the attack’s disruptive effects on national security, including the ability of defense installations and supporting civilian infrastructure to conduct operations abroad.<sup>264</sup> The *National Cyber Incident Response Plan* provides a framework for strengthening multisector coordination mechanisms for such attacks. As the administration refines the

plan, DOE and its government and industry partners should ensure that the issuance and execution of emergency orders fit within this broader framework and directly contribute to multisector resilience.

Updates to the *National Response Framework* and other FEMA-led initiatives can offer further benefits for grid security emergencies. In its after-action report from the 2017 hurricane season, FEMA noted that emergency managers and their private sector partners lack the multisector coordination mechanisms necessary to accelerate the restoration of electric power and other lifeline services.<sup>265</sup> The report called for FEMA to build “a cross-sector approach to the Agency’s planning, organizing, response, and recovery operations,” and revise current national-level planning frameworks to create a cross-sector emergency support function.<sup>266</sup> DOE and industry should partner to prioritize support for power sustainment and restoration within this broader initiative.

The *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans* provides a prime opportunity to embed cross-sector coordination efforts in regional incident response plans.<sup>267</sup> The annex calls for the development of regional plans to build resilience against extended multistate blackouts and ensure that interdependent sectors can accelerate power restoration while also countering threats to public health and safety.<sup>268</sup> In many areas of the United States, utilities are already helping DOE, FEMA, and their state and local partners build such plans for their regions. Cross-sector preparedness for grid security emergencies should become a key focus of future power outage incident planning efforts.

<sup>263</sup> 15 U.S.C. § 3363, (a).

<sup>264</sup> Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee*, 11.

<sup>265</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 13.

<sup>266</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 12–13.

<sup>267</sup> EIS Council, *E-PRO Handbook III*, 45.

<sup>268</sup> DHS, *Power Outage Incident Annex*, 77.

In all of these planning and operational coordination initiatives, DOE and other departments responsible for specific infrastructure sectors should examine how other federal emergency authorities might supplement those that apply to the energy sector. The communications sector provides one such opportunity. The president has extensive authorities to address national security and emergency preparedness telecommunications issues under the Communications Act, including the power to prioritize the use of communications capabilities and provide complying entities with legal and regulatory protections.<sup>269</sup> Executive Order 13618 assigns many of these authorities and associated responsibilities to federal departments and agencies. The secretary of commerce, for example, is responsible for developing plans and procedures for emergency use of radio frequencies and other communications systems.<sup>270</sup> The secretary of homeland security is responsible for overseeing the development, testing, and implementation of emergency communications capabilities.<sup>271</sup> Using these capabilities to support power restoration could be enormously helpful in grid security emergencies. Equivalent emergency authorities for other sectors could assist restoration as well. However, as with all such opportunities, effectively using these federal authorities will depend on extensive preplanning.

State governors are likely to invoke their own authorities to respond to grid security emergencies. Governors have primary responsibility for protecting the health and safety of their citizens. Cyber and physical attacks on the grid, especially if paired with strikes against communications systems and other interdependent sectors, could disrupt hospitals, water systems, and other assets on which their citizens rely. Governors in every state have the ability to declare emergencies and issue executive orders to help deal

with such threats to public health.<sup>272</sup> A growing number of states are also including utility representatives in their emergency operations centers, building collaborative plans and coordination mechanisms to respond to attacks on the grid, and preparing for state National Guard personnel to help utilities defend and restore the flow of power. These initiatives are bolstering overall preparedness for grid security emergencies. However, if multiple governors employ their own emergency authorities and implement state-level blackout response plans, it will be enormously difficult to coordinate their efforts with federal actions—including the issuance of DOE emergency orders to utilities in those very same states.

The only way to overcome such difficulties is to exercise the use of all of the authorities that could help protect and restore grid reliability, across multiple sectors and with the participation of both federal and state leaders. GridEx IV offered an important step forward in this regard. Exercise participants from the oil and natural gas subsector, as well as the financial-services and communications sectors, contributed perspectives on how they could help utilities respond to cyber and physical attacks on the grid. Representatives from state governments discussed how governors might act in such an emergency. GridEx V will provide an opportunity to address such coordination challenges in greater detail. GridEx V could also exercise the use of specific template emergency orders, together with communications mechanisms and playbooks developed for grid security emergencies. Additional exercises by BPS entities and their partners at all levels of government will also be vital to prepare for the implementation of such orders.

## Extended Partnership Requirements within the United States and Abroad

Congress implicitly imposed geographic constraints on the secretary's authority to issue emergency orders to protect the reliability of defense critical electric

<sup>269</sup> 47 U.S.C. § 606.

<sup>270</sup> Obama, *Executive Order—Assignment*, section 5.3.

<sup>271</sup> Obama, *Executive Order—Assignment*, section 5.2. See also DHS, "Emergency Communications."

<sup>272</sup> Orenstein and White, "Emergency Declaration Authorities."

infrastructure. The FPA limits such infrastructure to that which is located in the forty-eight contiguous states or the District of Columbia.<sup>273</sup> However, Alaska and Hawaii are home to vital grid-dependent military installations and supporting civilian infrastructure, including facilities for US continental ballistic missile defense and command and control of military operations in the Pacific region. Key defense installations also exist in Guam and other US territories. As the electric industry and DOE build preparedness for grid security emergencies, they should consider collaborating with the utilities that serve these states and territories and their government partners (including DOD) to strengthen plans and capabilities for coordinated operations.

Close coordination will also be necessary with Canada. The secretary of energy has no authority to issue emergency orders to power companies in other countries. However, the electric grids of the United States and Canada are deeply interconnected. This integration entails both risks and opportunities in grid security emergencies. Adversary-induced blackouts in one nation may cascade across the border, and extraordinary measures taken to restore US grid reliability could affect Canadian systems. Yet, the connectivity between US and Canadian electric systems can also provide unique opportunities to strengthen the security and emergency preparedness of both nations.

A key foundation for binational cooperation in grid security emergencies is already in place. NERC's reliability standards apply to both US and Canadian utilities, providing shared planning and emergency coordination mechanisms on both sides of the border. US and Canadian power companies and government officials should explore how they might supplement these existing mechanisms for

grid security emergencies. The most immediate opportunity to do so will lie in government-to-government consultations. The FPA requires that, to the extent practicable, the secretary of energy shall consult with Canadian authorities before issuing emergency orders.<sup>274</sup> However, the FPA provides no details on the mechanisms by which consultations will be conducted or on whether and how Canadian officials should be informed when the secretary issues emergency orders to US utilities. The analysis that follows examines opportunities to facilitate binational consultation and operational coordination in grid security emergencies.

The FPA also requires that the secretary consult with the Mexican government before issuing emergency orders. While the US and Mexican grids are much less integrated than those of the US and Canada, discussions on grid security emergency preparedness with Mexican officials could also be valuable. Coordination beyond North America may be useful as well. If a severe regional crisis escalates into attacks on the US power grid, US security partners in those regions may face strikes against their own electric systems. Sharing information on whether an attack is imminent and taking coordinated grid protection measures (including those for conservative operations) will help the United States and its allies meet such challenges.

### **Deepening Integration between US and Canadian Grids: Risks and Potential Benefits for Grid Security Emergency Resilience**

DOE notes that "the United States and Canada serve as a global model of highly functional, cross-border electricity coordination."<sup>275</sup> US and Canadian grids are connected by over three dozen major transmission lines, ranging from the Pacific Northwest to New England. The resulting power flows have created a deeply integrated network of north-south BPS infrastructure and synchronized

<sup>273</sup> 16 U.S.C. § 824o-1, (a)(4). The FPA's section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).

<sup>274</sup> 16 U.S.C. § 824o-1, (b)(3).

<sup>275</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-5.



cross-border operations.<sup>276</sup> This integration also provides significant economic and energy security benefits for both countries.<sup>277</sup>

Connectivity between US and Canadian grids will grow still closer in the decades to come.<sup>278</sup> New York and Massachusetts are pursuing significant increases in Canadian hydropower to help achieve their clean energy goals. Several new cross-border transmission lines are also under development, though many of them face permitting challenges. The Lake Erie Connector is a one-thousand-megawatt high-voltage, direct current line expected to link Ontario's Independent Electricity System Operator with PJM in 2020.<sup>279</sup> The Champlain Hudson Power Express from Quebec to New York City is expected to go into service in 2021, with still other projects in various phases of development in New England, the Midwest, and the Pacific Northwest.<sup>280</sup>

These and other projects offer significant economic benefits to both nations. However, the connectivity of US and Canadian power grids also creates risks of cross-border failures. The 2003 Northeast blackout that started in Ohio created power outages for millions of customers in Ontario.<sup>281</sup> Interconnections between US and Canadian power systems have increased since that event. US and Canadian officials warn that given this connectivity, "isolated or complex events with cascading effects that take place in either country can have major consequences for both the United States' and Canada's electric grids and adversely affect national security, economic stability, and public health and safety."<sup>282</sup>

Mandatory reliability standards reduce the risks of outages across North America. In the aftermath of the 2003 blackout, NERC began issuing standards applicable to entities on both sides of the border. NERC reliability standards are mandatory and enforceable in the provinces of Ontario, New Brunswick, Alberta, British Columbia, Manitoba, and Nova Scotia. Twelve such reliability standards also went into effect in Quebec in April 2015; the province is now considering adopting additional standards.<sup>283</sup> These shared US-Canada standards help power companies in both countries maintain the reliability of their systems and will help them prevent instabilities from spreading during grid security emergencies.

NERC's role as the electric reliability organization for North America provides an additional bulwark for binational grid resilience. As Figure 7 illustrates, three NERC regional entities include power companies on both sides of the border: the Northeast Power Coordinating Council (NPCC), the Midwest Reliability Organization (MRO), and the Western Electricity Coordinating Council (WECC). These entities help monitor and enforce compliance with reliability standards and reinforce NERC's integrated approach to reducing the risks of cascading failures and other instabilities.<sup>284</sup> The E-ISAC also provides additional support for utility preparedness in both nations.

However, Russia and other potential adversaries' increasingly sophisticated cyber capabilities pose challenges for protecting power flows between Canada and the United States, just as they do for electric service within each country individually.

Connectivity between US and Canadian power systems offers other benefits for protecting reliability against cyber and physical attacks. For example, as

<sup>276</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-6.

<sup>277</sup> Stanley, *Mapping the U.S.-Canada Energy Relationship*, 9.

<sup>278</sup> Parfomak et al., *Cross-Border Energy Trade*, 34.

<sup>279</sup> "Work Continues on ITC Lake Erie Project," *Transmission Hub*.

<sup>280</sup> Vine, *Interconnected: Canadian and U.S. Electricity*, 9.

<sup>281</sup> NERC Steering Group, *Technical Analysis of Blackout*, 1.

<sup>282</sup> Governments of US and Canada, *Joint United States-Canada Electric Grid Security and Resilience Strategy*, 10.

<sup>283</sup> "North America," NERC. See also "Compliance - Québec," Northeast Power Coordinating Council; and "Electric Power Transmission Reliability Standards," Régie de l'énergie Québec.

<sup>284</sup> "Key Players," NERC.



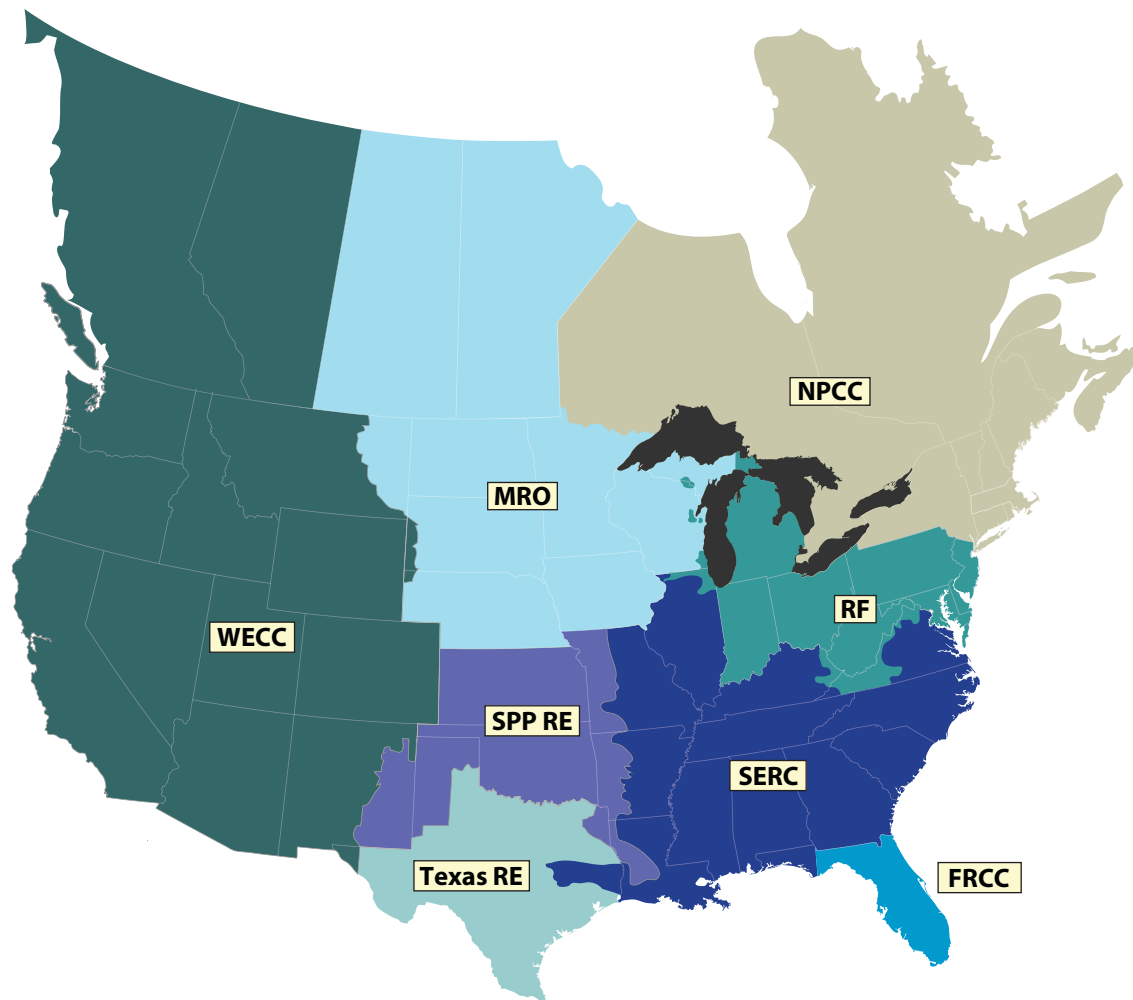


Figure 7. NERC Regional Entities across North America

new transmission lines increase this connectivity, electricity exported by Canada could become increasingly valuable when managing power imbalances in the United States and could make up for sudden shortfalls in the availability of US-generated power. However, we must assume that adversaries know this as well. To maximize the disruption to the US grid and the critical facilities that depend on it, attackers may strike the cross-border transmission lines that would otherwise help US grid owners and operators prevent cascading failures, uncontrolled separations, and other major reliability issues.

Adversaries may also attack grid assets that supply power to critical Canadian defense installations. The United States and Canada have a unique binational

defense system to protect their territories. The North American Aerospace Defense Command plays a vital role for both nations for aerospace warning, aerospace control, and maritime warning for North America.<sup>285</sup> The Canada-US Civil Assistance Plan also helps enable military members from one nation assist the other's armed forces in support of civilian authorities during emergencies.<sup>286</sup> Potential adversaries such as Russia may seek to degrade these binational military capabilities and operations by attacking defense critical electric infrastructure on

<sup>285</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

<sup>286</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

both sides of the border. US and Canadian officials and power companies should plan accordingly for mutual support in grid security emergencies.

### Specific Options for US–Canada Coordination

In addition to requiring US–Canada consultations before the secretary issues emergency orders, the FPA also states that FERC and the secretary “shall, in consultation with Canadian and Mexican authorities, develop protocols for the voluntary sharing of critical electric infrastructure information with Canadian and Mexican authorities and owners, operators and users of the bulk-power system outside the United States.”<sup>287</sup> Those initiatives provide a valuable starting point to build shared North American preparedness for grid security emergencies. However, much deeper collaboration is both possible and necessary, especially with Canada. Options for further analysis are described below.

**Consultative mechanisms, collaborative planning, and coordinated emergency operations.** The FPA does not specify how US officials would consult with their Canadian counterparts if the president declares a grid security emergency. Nor does it discuss whether the president would do so prior to making such a declaration. Exchanges between the US president and the prime minister of Canada would constitute the highest level of binational coordination. More detailed discussions about options for responding to incidents could also occur between the secretary of energy and the Canadian minister of national resources. That minister has the federal lead for electricity issues in Canada but lacks emergency authorities equivalent to those that the FPA grants to the secretary of energy.<sup>288</sup>

However, government coordination mechanisms will also need to include a broader array of participants. Global Affairs Canada and the US State Department might well be involved in any coordination of

binational grid emergency actions, just as they are in other emergency assistance mechanisms.<sup>289</sup> Coordination with state and provincial governments could also be helpful. The 1982 amendments to Canada’s Constitution Act (1867) explicitly recognized provinces’ and territories’ constitutional rights to manage electrical energy.<sup>290</sup> In particular, authority over electricity generation and transmission in Canada rests primarily with provincial governments.<sup>291</sup> It will be essential to account for these features of Canadian governance in building US–Canada consultative mechanisms.

The NERC alert system and other emergency coordination systems provide a solid basis for collaboration between US and Canadian utilities in grid security emergencies. However, the FPA does not address the question of how (and how much) information DOE officials should share with Canada on the issuance of emergency orders to US utilities. Given the deep integration of the US and Canadian grids, maximum sharing could help coordinate both countries’ emergency operations before, during, and after attacks. To facilitate such information sharing, DOE, Natural Resources Canada, and other relevant stakeholders can leverage existing US–Canadian mechanisms to protect sensitive information, supplemented as needed to support grid security emergency coordination.

The *Joint US-Canada Electric Grid Security and Resilience Strategy* (December 2016) provides a policy framework for building these coordination and information sharing mechanisms. The US and Canadian governments developed the strategy “to strengthen the security and resilience of the U.S. and Canadian electric grid from all adversarial, technological, and natural hazards and threats.”<sup>292</sup> The strategy calls for collaboration to protect system assets and

<sup>287</sup> 16 U.S.C. § 824o–1, (d)(5).

<sup>288</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>289</sup> “Compendium,” Public Safety Canada.

<sup>290</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>291</sup> “North America,” NERC.

<sup>292</sup> Governments of US and Canada, *US-Canada Electric Grid Security and Resilience Strategy*, 1.

critical functions in both nations so that the North American grid can “withstand and recover rapidly from disruptions.”<sup>293</sup> The strategy also emphasizes the need for collaboration to manage contingencies and enhance response and recovery efforts.<sup>294</sup> All of these features make the strategy a promising basis for creating the detailed collaborative mechanisms that grid security emergencies will require.

### **Protecting defense critical electric infrastructure.**

While the FPA facilitates the development of emergency orders to protect the flow of power to critical US defense installations, US–Canada coordination in grid security emergencies could also help strengthen power resilience for bases on both sides of the border. The Pacific Northwest exemplifies the potential benefits of such collaboration. Washington State hosts a number of vital installations, including Joint Base Kitsap on Puget Sound, which serves as the homeport for aircraft carriers, attack submarines, and other assets that would be needed for operations in the South China Sea and for other regional contingencies. Canadian Forces Base Esquimalt and other key Canadian installations are located less than one hundred miles away on Vancouver Island. Esquimalt is the second-largest military base in Canada and is home to Maritime Forces Pacific and Joint Task Force Pacific headquarters.<sup>295</sup> Coordinating US–Canada emergency plans to protect the flow of power to these installations could benefit the security of both nations.

The US–Canada Permanent Joint Board on Defense provides an ideal venue to explore such coordination options. Established in 1940 to discuss and advise on issues related to continental defense and security, the board has focused increasing attention on binational opportunities to strengthen critical infrastructure resilience. In 2011, the CEO of NERC led a

Permanent Joint Board on Defense discussion of how North American BPS emergency plans and coordination mechanisms could benefit US and Canadian national security. Natural Resources Canada and DOE have also participated in subsequent Permanent Joint Board on Defense meetings, along with the defense departments of both nations and critical infrastructure stakeholders. US and Canadian officials should consider using the board to facilitate industry–government discussions on opportunities to coordinate in grid security emergencies.

### **Coordination with Mexico and Beyond: Multinational Resilience against Grid Security Emergencies**

The US grid has much less connectivity with Mexican electric systems than with the Canadian grid. Southern California and a portion of Mexico’s Baja California have synchronous interconnections. Along the Mexico–Texas border, asynchronous interconnections also exist between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities.<sup>296</sup> In 2017, Mexican and US officials agreed to nonbinding pledges to increase this connectivity in ways that would strengthen reliability on both sides of the border.<sup>297</sup>

The election of Mexican president Andrés Manuel López Obrador in July 2018 may lead to significant changes in that country’s energy policies.<sup>298</sup> Structural challenges will also slow efforts to increase US–Mexico grid integration, including repeated power shortages and major shortfalls in the functionality of the Mexican grid.<sup>299</sup> Nevertheless, it could be useful to expand discussions with industry and the incoming government on protecting grid reliability against cyber and physical threats.

<sup>293</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 12.

<sup>294</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 11.

<sup>295</sup> “Maritime Forces Pacific,” Royal Canadian Navy.

<sup>296</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–4.

<sup>297</sup> “Increasing Electricity Cooperation in North America,” DOE.

<sup>298</sup> Kissane and Medina, “Energy Aftershocks.”

<sup>299</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–13.

Building grid security emergency coordination mechanisms beyond North America would also be helpful. As noted earlier, attacks on the US grid are most likely to occur in the context of an intense, escalating regional crisis in the Baltics, Northeast Asia, or some other area where US allies and critical security interests are at risk. In particular, adversaries may seek to inflict blackouts that could disrupt the deployment of US forces to the crisis zone. But we should also expect that US allies in the region will suffer attacks on their own grids, aimed at disrupting their ability to conduct combined operations with the United States and deliver electricity to US bases on their territories.

NATO's 2018 Locked Shields exercise focused on building alliance-wide preparedness for cyber and physical attacks against energy and communications systems.<sup>300</sup> In future exercises, allies might explore how to jointly determine whether grid attacks are potentially imminent and coordinate on the implementation of conservative operations across NATO member countries. The United States might explore equivalent opportunities for collaboration with Japan, South Korea, Australia, New Zealand, and other security partners. Existing treaty commitments, including those under Article V of NATO's founding treaty, will provide a starting point to meet our shared grid resilience challenges.<sup>301</sup>

### Playing Defense in Cyberwarfare: Doctrine, Integrated Planning, and Benefits for Deterrence

Utility leaders are urging the federal government to do more to assist them in deterring and defeating attacks on the grid. Their calls come at a perfect time. Administration officials have opened the door to new forms of operational collaboration between industry and government, including "collective

defense" during cyber attacks.<sup>302</sup> This report examines an especially significant option to expand their collaboration: coordinating the implementation of emergency orders with DOD operations to halt attacks at their source.

Deeper operational partnerships can also help meet underlying challenges for cyber deterrence. A number of cybersecurity analysts argue that deterrence by denial is impractical in cyberspace because offensive cyber capabilities are so much stronger than cyber defenses, and because cyber warfare will be very different from conventional conflicts. Analysts also warn that the United States lives in a cyber "glass house": given the vulnerability of the power grid and other infrastructure systems, the president cannot credibly threaten to use cyber weapons to defend US allies and interests. Improving preparedness for grid security emergencies can help address these concerns and support ongoing reassessments of US strategies for deterrence.

### Unity of Effort in Defensive Operations at Home and Abroad

Tom Fanning, CEO of Southern Company (one of the largest power companies in the United States), notes that he and other infrastructure owners and operators face a major constraint on their ability to defend their systems: "I can't fight back."<sup>303</sup> In theory, blunting attacks at their source could greatly ease the scale and severity of the threats that utilities will need to counter. In practice, integrating grid security emergency operations with measures to suppress enemy attacks would entail major policy and technical obstacles.

Power companies should not be responsible for striking enemies' offensive cyber infrastructure during grid security emergencies. The US government is the sole actor with the prerogative to engage in techniques such as "hacking back" that

<sup>300</sup> Cowan, "Locked Shields 2018."

<sup>301</sup> "The North Atlantic Treaty," NATO.

<sup>302</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>303</sup> Smith, "U.S. Officials Push New Penalties."



involve operations to disrupt or destroy an attacker's system.<sup>304</sup> Moreover, even if power companies gained legal authority to fight back against adversaries, their technical capacity to do so would be dwarfed by the capabilities possessed by US Cyber Command and other US government organizations.

Efforts to integrate defensive operations at home and abroad should rest on the comparative advantages of industry and government. BPS entities and other components of the electricity subsector are best positioned to defend their systems from within, assisted by DOE and other government partners. Operations abroad to halt attacks on the grid should remain the exclusive purview of government agencies, supported by industry assistance to gather malware samples and facilitate attack attribution. Based on this division of labor, government and industry leaders could explore whether and how to strengthen unity of effort for the full scope of defensive operations within the United States and beyond.

Secretary of homeland security Kirstjen Nielsen has called for the adoption of a "collective defense" posture that might include such expanded partnerships. Under the collective defense model, industry and government would collaborate to act on threat indicators and "respond more quickly and effectively to incidents."<sup>305</sup> The most familiar realm of operational collaboration lies in government support to help utilities detect, characterize, and eradicate malware on their systems. DHS is strengthening the National Cybersecurity and Communications Integration Center's ability to provide such assistance.<sup>306</sup> State National Guard organizations can also support post-cyber attack power restoration within the larger context of the industry's Cyber Mutual Assistance system.<sup>307</sup> However, in a cyber strike against the

United States, DOD will require many of these same guard personnel to protect the department's networks, conduct cyber operations against the attacker, and carry out other federal missions.<sup>308</sup> Power companies and government agencies will need to continue clarifying whether and how specific National Guard assets can help meet utility requests for assistance; existing doctrine and procedures for providing defense support to civil authorities offer a solid basis to advance those discussions.

In contrast, coordinating industry grid protection measures with government operations to suppress attacks would extend collective defense into uncharted territory. The command vision for US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, offers a starting point to examine how engaging against malicious cyber actors might help protect utilities. The document states that the United States must "increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage." To do so, DOD "is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems."<sup>309</sup>

Forward defense operations could respond to and help counter adversary efforts to implant malware on utility networks. Should such operations also help power companies protect their systems if the president declares that an attack is imminent? As senator Mike Rounds frames the question: "If someone is going to shoot an arrow at you, do you shoot the archer before he shoots the arrow?"<sup>310</sup>

US Cyber Command's vision statement does not directly address this possibility. However, each phase of grid security emergencies will likely offer

<sup>304</sup> GWU, *Into the Gray Zone*, 25.

<sup>305</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>306</sup> Marks, "DHS Stands Up New Cyber Risk Center."

<sup>307</sup> Crowe, "National Guard Preparing"; and Puryear, "91st Cyber Brigade Activated."

<sup>308</sup> DOD, *Cyber Strategy*, 4.

<sup>309</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 4–5.

<sup>310</sup> Bordelon, "Rounds Is Ready."



a different mix of risks and rewards for combining domestic and forward defense operations. For example, if the president determines that an attack on the grid is imminent, the secretary might issue orders for conservative operations to bolster grid defenses at the same moment that forward defense operations disrupted enemy cyber infrastructure poised to launch the strike. But assessments that an attack is imminent may turn out to be wrong. No-regrets orders for conservative operations are valuable precisely because using them will entail few consequences if warning indicators turn out to be false. Preattack forward defense operations could start a cyberwar that might not otherwise have occurred.

The United States can avoid such risks by waiting until attacks on the grid are under way before striking the enemy's offensive infrastructure. However, developing the technical capabilities to identify and disrupt the cyber infrastructure being used in an attack could prove challenging. Moreover, it is not clear whether integrating plans for home and away operations would offer significant benefits, as opposed to relying on utilities and government agencies to conduct those two types of operations independently.

US Cyber Command has opened the door to building new types of partnerships with the electricity subsector. The command has called for measures to "deepen and operationalize" collaboration between the private sector, the armed services, and other command partners.<sup>311</sup> As those efforts go forward with the electricity subsector and DOE, exploring options for collective defense (and clarifying the dangers they might present) should be a prime focus for analysis.

### **Maximizing Industry Contributions to Cyber Deterrence by Denial**

The *National Security Strategy* emphasizes that rather than rely on threats of cost imposition alone

to deter enemy attacks, the United States will also strengthen deterrence by denial. This report has examined how grid security emergency orders and implementation plans can raise adversaries' doubts as to whether they can achieve their objectives. But strengthening this form of deterrence will also entail underlying challenges.

Many cybersecurity analysts believe that offensive cyber capabilities are vastly stronger than defenses against them, and that this preeminence creates destabilizing incentives for adversaries to strike first when conflicts loom.<sup>312</sup> Unless measures to strengthen grid resilience can help weaken the dominance of offense over defense in the cyber realm, deterrence by denial will remain difficult to accomplish against highly capable adversaries.

However, today's offensive dominance stems in part from historical factors that are rapidly changing. The interconnected grid evolved decades ago when no cyber threat existed to drive protective measures. Moreover, as utilities began incorporating computer-assisted controls, sensors, and operating technology systems, few of these companies accounted for the risk that cyber threats to their systems would escalate so rapidly. As noted in this report, utilities are advancing a wide array of technical initiatives and fallback operational plans to counter and (ideally) stay ahead of adversaries' capabilities. In addition, regulatory bodies across the nation are increasingly willing to enable companies to recover costs for cyber resilience.

The current preeminence of offense over defense also reflects organizational factors. Rebecca Slayton has found that historically, "the success of offense is largely the result of a poorly managed defense."<sup>313</sup> The skills of the individuals employing cyber weapons and defensive tools, and the effectiveness with which

<sup>311</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 8.

<sup>312</sup> For a review of this "offense-dominant" literature, and the smaller set of works opposing it, see Slayton, "What Is the Cyber Offense-Defense Balance?," 72.

<sup>313</sup> Slayton, "What Is the Cyber Offense-Defense Balance?," 87.

these practitioners are managed and organized, have an enormous impact on the outcome of cyber engagements. Slayton notes that the importance of organization for cyber defense is implicit in discussions of the need for better public-private partnerships and information sharing. What has been missing, however, are efforts to make such partnerships *operational* and create unity of effort in government-industry defense actions when adversaries strike. That is precisely the gap that DOE and its industry partners can fill by developing grid security emergency orders and advancing all of the other collaborative initiatives necessary to make those orders effective.

Improved partnerships and technical capabilities to protect the grid cannot by themselves make defense preeminent. To further rebalance offense and defense in cyberspace, resilience initiatives will be necessary across all critical infrastructure sectors, as well as a host of other measures to facilitate the command, control, and coordination of public-private defensive operations. But building preparedness for grid security emergencies will be vital for that broader effort. Moreover, establishing defensive primacy is not necessary to facilitate deterrence by denial. As defined by the *National Security Strategy*, deterrence by denial functions by creating doubt in our adversaries that they can achieve their objectives.<sup>314</sup> DOE and its partners should develop grid security emergency orders that (perhaps in conjunction with forward defense operations) can make adversaries less likely to attack, even if defensive dominance remains out of reach.

Strengthening grid resilience can also support the broader reassessment of the US deterrence posture that is now under way. Robert Strayer, the State Department's deputy assistant secretary for cyber and international communications and information policy, notes that the increasing severity of threats to

US infrastructure is forcing "an evolution in the US government's thinking about how to deter malicious cyber actors."<sup>315</sup> In conventional warfare, deterrence by denial functions by making it physically difficult for adversaries to achieve their objectives and by raising enemy forces' costs of taking their targets.<sup>316</sup> Cyberwarfare will not entail the same sorts of attrition of enemy forces that occurs in battles with tanks, fighter aircraft, and other conventional weapons. The Trump and Obama administrations have redefined deterrence by denial to better fit the characteristics of cyberspace. The unique features of cyber conflict will require continued rethinking of how the United States can strengthen deterrence in the years to come. As utilities and government agencies build resilience for grid security emergencies, new opportunities will emerge to influence adversaries' perceived costs and benefits of attack. The United States should continue to refine its deterrence posture to capitalize on these improvements.

### Escaping the "Glass House" Syndrome

The president may need the ability to use cyber weapons against foreign targets to help resolve crises on terms favorable to the United States. The *DOD Cyber Strategy* (April 2015) states that:

There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an

<sup>314</sup> White House, *National Security Strategy*, 13.

<sup>315</sup> Smith, "U.S. Officials Push New Penalties."

<sup>316</sup> For definitions of classic deterrence by denial derived from conventional warfare, see Gerson, "Conventional Deterrence"; and Mitchell, "The Case for Deterrence by Denial." For an analysis of how that definition differs from that used by the Trump administration, see Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy."

ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests.<sup>317</sup>

However, any such operations against an adversary's cyber infrastructure would risk retaliatory strikes against the United States—including, potentially, attacks on the grid. Senator Thom Tillis (R-NC), a member of the Senate Armed Service Committee, emphasizes that the United States is living in “a big glass house.”<sup>318</sup> If US infrastructure owners and operators cannot defend their systems against attack, the president may be reluctant to use cyber weapons abroad, even if doing so might otherwise offer enormous benefits for conflict termination. In short: US leaders may be self-deterred from taking actions that they may need to employ. Developing emergency orders and implementation plans to protect grid reliability could reduce these glass house constraints and widen the range of options available for the president to protect US interests.

Improving grid defenses could also help strengthen the credibility of US commitments to defend key allies. Former US defense and intelligence officials have proposed that the United States and other high-cyber-capability NATO allies provide extended deterrence against cyber attacks for less capable alliance members.<sup>319</sup> But glass house concerns would call into question the credibility such commitments. Measures to strengthen grid resilience could help convince adversaries that the United States is willing to help allies respond to cyber attacks on their infrastructure.

Yet, nothing requires the United States to respond to such attacks with cyber weapons alone. On the contrary: the *National Security Strategy* and other policy documents leave open the possibility that

if cyber attacks at home or abroad are sufficiently severe, the United States will respond with conventional or even nuclear weapons. James Lewis notes that “opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return,” and will surely weigh that risk given “the immense capacity of the United States to inflict punishment” on attackers.<sup>320</sup> Emergency orders to protect the flow of power to defense installations can and should reinforce the certainty of that punishment.

But any first use of cyber weapons by the United States would entail escalatory dangers as well. If the United States were to initiate the use of destructive cyber weapons to defend US allies and interests, potential adversaries such as Russia could respond with conventional or nuclear forces. Moreover, conflicts that begin with the large-scale use of cyber weapons could also spiral out of control in ways that neither side desires or anticipates.<sup>321</sup> These escalatory risks must be in the forefront of calculations on whether and how to engage in cyber warfare. Indeed, as government agencies partner with power companies to build resilience for grid security emergencies, deterring such conflicts and reducing the likelihood of cyberwarfare should always be our prime objective.

<sup>317</sup> DOD, *Cyber Strategy*, 5.

<sup>318</sup> Schwartz, “Sen. Tillis: We Are Living in a Glass House.” For additional analysis of the glass house syndrome and its effects on constraining US options, see Miller, “Cyber Deterrence”; and Rosenbach, “Living in a Glass House.”

<sup>319</sup> Kramer, Butler, and Lotrionte, *Cyber, Extended Deterrence, and NATO*, 1.

<sup>320</sup> Lewis, *Rethinking Cybersecurity*, 9, 29. The author also argues that even if attacks on the grid occur, they would be unlikely to achieve the strategic effects that adversaries will seek, further reducing the likelihood of such attacks (see pp. 21 and 24–26).

<sup>321</sup> Danzig, *Surviving on a Diet of Poisoned Fruit*, 25; Lin, “Escalation Dynamics,” 52; and Miller and Fontaine, *A New Era*, 18–20.

## Bibliography

- 6 U.S.C. § 124l. <https://www.law.cornell.edu/uscode/text/6/124l>.
- 15 U.S.C. § 3361. <https://www.law.cornell.edu/uscode/text/15/3361>.
- 15 U.S.C. § 3363. <https://www.law.cornell.edu/uscode/text/15/3363>.
- 15 U.S.C. § 3364. <https://www.law.cornell.edu/uscode/text/15/3364>.
- 16 U.S.C. § 824a. <https://www.law.cornell.edu/uscode/text/16/824a>.
- 16 U.S.C. § 824o. <https://www.law.cornell.edu/uscode/text/16/824o>.
- 16 U.S.C. § 824o–1. <https://www.law.cornell.edu/uscode/text/16/824o–1>.
- 18 CFR 388.113. <https://www.law.cornell.edu/cfr/text/18/388.113>.
- 47 U.S.C. § 606. <https://www.law.cornell.edu/uscode/text/47/606>.
- 50 U.S.C. Appendix §2071(c). <https://law.justia.com/codes/us/2001/title50/app/defensepr/sec2071/>.
- “About Alerts.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx>.
- “About NERC.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/AboutNERC/Pages/default.aspx>.
- “About NSTAC.” DOS (US Department of State). Last published June 20, 2016. <https://www.dhs.gov/about-nstac>.
- “About 60% of the U.S. Electric Power Supply Is Managed by RTOs.” US Energy Information Administration. April 4, 2011. <https://www.eia.gov/todayinenergy/detail.php?id=790>.
- “Alert (ICS-ALERT-14-281-01E): Ongoing Sophisticated Malware Campaign Compromising ICS (Update E).” ICS-CERT. Originally released December 10, 2014, last revised December 9, 2016. <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.
- “Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure.” ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). February 25, 2016. <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.
- “Alert (TA17-163A): CrashOverride Malware.” US-CERT (US Computer Emergency Readiness Team). June 12, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-163A>.
- “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). October 20, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-293A>.
- “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). March 15, 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.



- ASD(EI&E) (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment). *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*. Washington, DC: DOD, July 2017. <https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf>.
- Assante, Michael, and Robert M. Lee. *The Industrial Control System Cyber Kill Chain*. Bethesda, MD: SANS Institute, October 2015. <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.
- “Automated Indicator Sharing (AIS).” US-CERT (US Computer Emergency Readiness Team). n.d. <https://www.us-cert.gov/ais>.
- Banham, Russ. “DDoS Attacks Evolve to Conscript Devices onto the IoT.” *Forbes*, February 4, 2018. <https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#4b5a43a86aaa>.
- Barnes, Julian E. “‘Warning Lights Are Blinking Red,’ Top Intelligence Officer Says of Russian Attacks.” *New York Times*, July 13, 2018. <https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html>.
- Blue Ribbon Study Panel on Biodefense (Hudson Institute). *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts—A Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*. Washington, DC: Hudson Institute, October 2015. <http://www.biodefensestudy.org/a-national-blueprint-for-biodefense>.
- Bordelon, Brendan. “Rounds Is Ready to Lead New Senate Cybersecurity Subcommittee.” *Morning Consult*, February 1, 2017. <https://morningconsult.com/2017/02/01/rounds-ready-lead-new-senate-cybersecurity-subcommittee/>.
- Brown, Jared T., and Daniel H. Else. *The Defense Production Act of 1950: History, Authorities, and Reauthorization*. Washington, DC: Congressional Research Service, July 28, 2014. <https://fas.org/sgp/crs/natsec/R43118.pdf>.
- “The Canada-U.S. Defence Relationship.” Department of National Defence and the Canadian Armed Forces. December 4, 2014, last modified February 10, 2015. <http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s>.
- Cherepanov, Anton, and Robert Lipovsky. “Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet.” *WeLiveSecurity* (ESET Blog), June 12, 2017. <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.
- “Compendium of U.S.-Canada Emergency Management Assistance Mechanisms.” Public Safety Canada. October 2016, last modified March 28, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cmpndm-ntdstts-cnd-2016/index-en.aspx>.
- “Compliance - Québec.” Northeast Power Coordinating Council. n.d. <https://www.npcc.org/Compliance/Quebec/Forms/Public%20List.aspx>.
- Cowan, Gerrard. “Locked Shields 2018 Practises for Large-Scale Cyber Incident.” *Jane’s 360*, April 29, 2018. <http://www.janes.com/article/79652/locked-shields-2018-practises-for-large-scale-cyber-incident>.



- Crowe, Greg. "National Guard Preparing to Defend Cyberspace for States." *Federal News Radio*, April 16, 2018. <https://federalnewsradio.com/cyber-exposure/2018/04/national-guard-preparing-to-defend-cyberspace-for-states/>.
- "Cybersecurity." American Gas Association. n.d. <https://www.aga.org/safety/security/cybersecurity/>.
- "The Cyber Threat Framework." ODNI (Office of the Director of National Intelligence). n.d. <https://www.dni.gov/index.php/cyber-threat-framework>.
- Danzig, Richard. *Catastrophic Bioterrorism—What Is to Be Done?* Washington, DC: Center for Technology and National Security Policy, August 2003. [http://www.response-analytics.org/images/Danzig\\_Bioterror\\_Paper.pdf](http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf).
- . *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Washington, DC: Center for a New American Security, July 2014. [https://s3.amazonaws.com/files.cnas.org/documents/CNAS\\_PoisonedFruit\\_Danzig.pdf](https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf).
- Defense Science Board. *Task Force on Cyber Deterrence*. Washington, DC: DOD, February 2017. [https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport\\_02-28-17\\_Final.pdf](https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf).
- DHS (US Department of Homeland Security). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: DHS, December 17, 2003. <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- . *National Cyber Incident Response Plan*. Washington, DC: DHS, December 2016. [https://www.us-cert.gov/sites/default/files/ncirp/National\\_Cyber\\_Incident\\_Response\\_Plan.pdf](https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf).
- . *National Response Framework*. 3rd ed. Washington, DC: DHS, June 2016. [https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National\\_Response\\_Framework3rd.pdf](https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf).
- . *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS, 2013. <https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf>.
- . *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage*. Washington, DC: DHS, June 2017. <https://www.fema.gov/media-library/assets/documents/154058>.
- . *Strategy for Protecting and Preparing the Homeland against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*. Washington, DC: DHS, forthcoming.
- . *U.S. Department of Homeland Security Cybersecurity Strategy*. Washington, DC: DHS, May, 15, 2018. [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf).
- DiSavino, Scott, and David Sheppard. "ConEd Cuts Power to Part of Lower Manhattan Due to Sandy." *Reuters*, October 29, 2012. <https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030>.

- DOD (US Department of Defense). *Department of Defense Manual 3020.45*. Washington, DC: DOD, last updated May 23, 2017. <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>.
- . *DoD Cybersecurity Discipline Implementation Plan*. Washington, DC: DOD, amended February 2016. <http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf>.
- . *DOD Cyber Strategy*. Washington, DC: DOD, April 2015. [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).
- . *DoD Directive 3020.40: Mission Assurance (MA)*. Washington, DC: DOD, November 29, 2016. [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).
- . *Mission Assurance Strategy*. Washington, DC: DOD, April 2012. [http://policy.defense.gov/Portals/11/Documents/MA\\_Strategy\\_Final\\_7May12.pdf](http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf).
- DOE (US Department of Energy). “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40).” *Federal Register* 83, no. 7 (2018): 1176. <https://www.federalregister.gov/documents/2018/01/10/2018-00259/grid-security-emergency-orders-procedures-for-issuance>.
- . *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. Version 1.1. Washington, DC: DOE, February 2014. <https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf>.
- . *Electromagnetic Pulse Resilience Action Plan*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf>.
- . “Energy Priorities and Allocations System Regulations (RIN 1901–AB28).” *Federal Register* 76, no. 111 (2011): 33615. <https://www.gpo.gov/fdsys/pkg/FR-2011-06-09/pdf/2011-14282.pdf>.
- . *Multiyear Plan for Energy Sector Cybersecurity*. Washington, DC: DOE, March 2018. [https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20\\_0.pdf](https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf).
- . *Quadrennial Energy Review—Transforming the Nation’s Electricity System: The Second Installment of the QER*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>.
- . *Staff Report to the Secretary on Electricity Markets and Reliability*. Washington, DC: DOE, August 2017. [https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability\\_0.pdf](https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability_0.pdf).
- . *Strategic Transformer Reserve: Report to Congress*. Washington, DC: DOE, March 2017. <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.
- “DOE’s Use of Federal Power Act Emergency Authority.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use>.

- DOS (US Department of State). *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. Washington, DC: DOS, May 31, 2018. <https://www.state.gov/documents/organization/282253.pdf>.
- Dougherty, Jon. “Biggest U.S. Power Grid Operator Suffers Thousands of Attempted Cyber Attacks per Month.” *Forward Observer*, August 28, 2017. <https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/>.
- Douris, Constance. “DARPA Research Leads Grid Security Solutions.” *The Buzz* (blog), *National Interest*, January 12, 2017. <http://nationalinterest.org/blog/the-buzz/darpa-research-leads-grid-security-solutions-19044>.
- Dragos, Inc. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. Hanover, MD: Dragos, June 13, 2017. <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>.
- EEI (Edison Electric Institute). “Comments of the Edison Electric Institute.” In *Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*. February 6, 2017.
- . *Understanding the Electric Power Industry’s Response and Restoration Process*. Washington, DC: EEI, October 2016. [http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA\\_101FINAL.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf).
- EIS Council (Electric Infrastructure Security Council). *E-PRO Handbook II: Volume 1—Fuel*. Washington, DC: EIS Council, 2016. [https://www.eiscouncil.org/App\\_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf](https://www.eiscouncil.org/App_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf).
- . *E-PRO Handbook III: Black Sky Cross-Sector Coordination and Communication*. Washington, DC: EIS Council, June 2018. [https://www.eiscouncil.org/EPRO\\_Books.aspx](https://www.eiscouncil.org/EPRO_Books.aspx).
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS-ICS. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Washington, DC: NERC, March 2016. [https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_18Mar2016.pdf](https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf).
- “Electricity Information Sharing and Analysis Center.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.
- “Electric Power Transmission Reliability Standards Compliance Monitoring and Enforcement.” Régie de l’énergie Québec. n.d. <http://www.regie-energie.qc.ca/en/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html>.
- “Emergency Communications.” DHS (US Department of Homeland Security). Last published June 26, 2018. <https://www.dhs.gov/topic/emergency-communications>.
- Energy Policy Act of 2005. Public Law 109-58. *U.S. Statutes at Large* 119 (2005): 942–943. <https://www.gpo.gov/fdsys/pkg/STATUTE-119/pdf/STATUTE-119.pdf>.
- “Energy Sector Cybersecurity Preparedness.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

- EPRI (Electric Power Research Institute). *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research*. Report 3002000796. Palo Alto, CA: EPRI, December 2013. <https://publicdownload.epri.com/PublicDownload.svc/product=000000003002000796/type=Product>.
- . *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs*. Report 3002008999. Palo Alto, CA: EPRI, September 2016. <https://www.epri.com/#/pages/product/000000003002008999/?lang=en>.
- ESCC (Electricity Subsector Coordinating Council). *Electricity Sub-Sector Coordinating Council Charter*. Washington, DC: DHS, August 5, 2013. <https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf>.
- “ESCC: Electricity Subsector Coordinating Council.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.
- “The ESCC’s Cyber Mutual Assistance Program.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1>.
- FEMA (US Federal Emergency Management Agency). *2017 Hurricane Season FEMA After-Action Report*. Washington, DC: FEMA, July 12, 2018. <https://www.fema.gov/media-library/assets/documents/167249>.
- FERC (Federal Energy Regulatory Commission). *Cyber Security Incident Reporting Reliability Standards*. 161 FERC ¶ 61,291. December 21, 2017. <https://www.ferc.gov/whats-new/comm-meet/2017/122117/E-1.pdf>.
- . *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies, Statement of Policy*. 96 FERC ¶ 61,299. September 14, 2011.
- . *Grid Resilience in Regional Transmission Organizations and Independent System Operators*. 162 FERC ¶ 61,256. 2018. <https://www.ferc.gov/CalendarFiles/20180320102618-AD18-7-000.pdf>.
- . *Order Authorizing Acquisition and Disposition of Jurisdictional Facilities*. 163 FERC ¶ 61,005. April 3, 2018. <https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf>.
- . *Order Granting Approvals in Connection with the Dissolution of the Southwest Power Pool Regional Entity*. 163 FERC ¶ 61,094. May 4, 2018. <https://www.ferc.gov/CalendarFiles/20180504141902-RR18-3-000.pdf>.
- . *Policy Statement on Matters Related to Bulk Power System Reliability*. 107 FERC ¶ 61,052. April 19, 2004. <https://www.ferc.gov/whats-new/comm-meet/041404/E-6.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833. 157 FERC ¶ 61,123. November 17, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-4.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833-A. 163 FERC ¶ 61,125. May 17, 2018. <https://www.ferc.gov/whats-new/comm-meet/2018/051718/E-2.pdf>.



- . *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*. 156 FERC ¶ 61,215. September 22, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/092216/E-4.pdf>.
- . *Revision to Electric Reliability Organization Definition of Bulk Electric System*. Order No. 743. 133 FERC ¶ 61,150. November 18, 2010. <https://www.ferc.gov/whats-new/comm-meet/2010/111810/E-2.pdf>.
- . *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*. Order No. 773-A. 143 FERC ¶ 61,053. April 18, 2013. <https://www.ferc.gov/whats-new/comm-meet/2013/041813/E-9.pdf>.
- FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation). *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*. Washington, DC: FERC, January 2016. <https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Further Joint Study Report: Planning Restoration Absent SCADA or EMS (PRASE)*. Washington, DC: FERC, June 2017. <https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Recommended Study: Blackstart Resources Availability (BRAv)*. Washington, DC: FERC, May 2018. <https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf>.
- Fischerkeller, Michael P., and Richard J. Harknett. “Deterrence Is Not a Credible Strategy for Cyberspace.” *Orbis* 61, no. 3 (2017): 381–393. <https://www.sciencedirect.com/science/article/pii/S0030438717300431>.
- Fixing America’s Surface Transportation Act, Public Law 114-94. *U.S. Statutes at Large* 129 (2015): 1773–1774. <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.
- Frankel, Alison. “Can Customers Sue Power Companies for Outages? Yes, but It’s Hard to Win.” *Reuters* (blog), November 9, 2012. <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>.
- Galloway, T. J., Sr. “Advancing Reliability and Resilience of the Grid.” Comments presented at the FERC Reliability Technical Conference, Washington, DC, July 31, 2018. <https://www.ferc.gov/CalendarFiles/20180731084251-Galloway,%20North%20American%20Transmission%20Forum.pdf>.
- Gerson, Michael S. “Conventional Deterrence in the Second Nuclear Age.” *Parameters* 39 (Autumn 2009): 32–48. <https://ssi.armywarcollege.edu/pubs/parameters/articles/09autumn/gerson.pdf>.
- Governments of the US and Canada. *Joint United States-Canada Electric Grid Security and Resilience Strategy*. Washington, DC: The White House, December 2016. [https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint\\_US\\_Canada\\_Grid\\_Strategy\\_06Dec2016.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf).
- GWU (George Washington University) Center for Cyber and Homeland Security. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: GWU, October 2016. <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf>.
- Healy, Jason. *The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities*. SSRN, June 2016. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2836206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206).



- Homeland Security Advisory Council. *Final Report of the Cybersecurity Subcommittee: Part I—Incident Response*. Washington, DC: DOS, June 2016. <https://www.hsd.org/?view&did=794271>.
- ICF. *Assessment of Large Power Transformer Risk Mitigation Strategies*. Fairfax, VA: ICF, October 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf>.
- . *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. Fairfax, VA: ICF, June 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>.
- “Increasing Electricity Cooperation in North America.” DOE (US Department of Energy). January 11, 2017. <https://www.energy.gov/policy/articles/increasing-electricity-cooperation-north-america>.
- INL (Idaho National Laboratory). *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*. Idaho Falls, IN: INL, January 2016. <https://inldigitallibrary.inl.gov/sites/STI/STI/INL-EXT-15-35582.pdf>.
- ISO-NE (ISO New England). *Operational Fuel-Security Analysis*. Holyoke, MA: ISO-NE, January 17, 2018. [https://www.iso-ne.com/static-assets/documents/2018/01/20180117\\_operational\\_fuel-security\\_analysis.pdf](https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf).
- . “Response of ISO New England Inc.” *Response to Grid Resilience in Regional Transmission Organization and Independent System Operators* (AD18-7-000). March 9, 2018. [https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7\\_iso\\_response\\_to\\_grid\\_resilience.pdf](https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7_iso_response_to_grid_resilience.pdf).
- Jenkins, Brian Michael. “Countering al-Qaeda: The Next Phase in the War.” *The RAND Blog*, September 8, 2002. <https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html>.
- Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*. Joint Publication 1. Washington, DC: Joint Chiefs of Staff, July 12, 2017. [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1\\_ch1.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf).
- Joint Commenters. “Comments of American Public Power Association, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group.” In *Response to RIN 1901-AB40*. February 23, 2017. <http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf>.
- Kaften, Cheryl. “DoD Tests Energy Continuity with ‘Islanded’ Microgrid.” *Energy Manager Today*, April 5, 2017. <https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/>.
- Kappenman, John. *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*. Goleta, CA: Metatech, January 2010. [https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc\\_meta-r-319.pdf](https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf).
- “Key Players.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>.
- Kissane, Carolyn, and Emily Medina. “Energy Aftershocks in Store after Seismic Mexican Election.” *The Hill*, July 3, 2018. <http://thehill.com/opinion/energy-environment/395383-energy-aftershocks-in-store-after-seismic-mexican-election>.

- Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte. *Cyber, Extended Deterrence, and NATO*. Washington, DC: Atlantic Council, May 2016. [http://www.atlanticcouncil.org/images/publications/Cyber\\_Extended\\_Deterrence\\_and\\_NATO\\_web\\_0526.pdf](http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf).
- Lawrence, Bill, Charlotte de Seibert, and Philip Daigle. "E-ISAC Update." Presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, FL, March 6–7, 2018. <https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf>.
- Lazar, Jim. *Electricity Regulation in the US: A Guide*. 2nd ed. Montpelier, VT: Regulatory Assistance Project, June 2016. <http://www.raponline.org/wp-content/uploads/2016/07/rap-lazar-electricity-regulation-US-june-2016.pdf>.
- Lewis, James A. "North Korea and Cyber Catastrophe—Don't Hold Your Breath." *38 North*, January 12, 2018. <http://www.38north.org/2018/01/jalewis011218/>.
- . *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Washington, DC: CSIS, January 2018. [http://espas.eu/orbis/sites/default/files/generated/document/en/180108\\_Lewis\\_ReconsideringCybersecurity\\_Web.pdf](http://espas.eu/orbis/sites/default/files/generated/document/en/180108_Lewis_ReconsideringCybersecurity_Web.pdf).
- Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. [http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06\\_Issue-3/Fall12.pdf](http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-3/Fall12.pdf).
- Lucas, Todd. "Conservative Operations." Presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, CO, September 18–19, 2013. <http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf>.
- Lynch, Justin. "How the Russian Government Allegedly Attacks the American Electric Grid." *Fifth Domain*, July 24, 2018. <https://www.fifthdomain.com/critical-infrastructure/2018/07/24/how-the-russian-government-attacks-the-american-electric-grid/>.
- Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (Sept./Oct. 2010). <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.
- "Maritime Forces Pacific." Royal Canadian Navy. Last modified November 24, 2016. <http://www.navy-marine.forces.gc.ca/en/about/structure-marpac-home.page>.
- Marks, Joseph. "DHS Stands up New Cyber Risk Center to Protect High-Value Targets." *Nextgov*, July 31, 2018. <https://www.nextgov.com/cybersecurity/2018/07/dhs-stands-new-cyber-risk-center-protect-high-value-targets/150179/>.
- Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn. *Power Begins at Home: Assured Energy for U.S. Military Bases*. Reston, VA: Noblis, January 12, 2017. [http://www.pewtrusts.org/~media/assets/2017/01/ce\\_power\\_begins\\_at\\_home\\_assured\\_energy\\_for\\_us\\_military\\_bases.pdf](http://www.pewtrusts.org/~media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf).
- McElwee, Steven. "Probabilistic Cluster Ensemble Evaluation for Unsupervised Intrusion Detection." Unpublished thesis, Nova Southeastern University, forthcoming.

- McElwee, Steven, Jeffrey Heaton, James Fraley, and James Cannady. "Deep Learning for Prioritizing and Responding to Intrusion Detection Alerts." In *2017 IEEE Military Communications Conference Proceedings*. Piscataway, NJ: IEEE, 2017. <https://ieeexplore.ieee.org/document/8170757/>.
- McGhee, Michael. "EEI Executive Advisory Committee." Slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017. [http://www.asaie.army.mil/Public/ES/oei/docs/EEI\\_Exec-Committee.pdf](http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf).
- Miller, James N. "Cyber Deterrence Cannot Be One Size Fits All." *Cipher Brief*, August 3, 2017. [https://www.thecipherbrief.com/column\\_article/cyber-deterrence-cannot-be-one-size-fits-all-1092](https://www.thecipherbrief.com/column_article/cyber-deterrence-cannot-be-one-size-fits-all-1092).
- Miller, James N., and James R. Gosler. "Memorandum for the Chairman, Defense Science Board" (preamble). In *Task Force on Cyber Deterrence*. Washington, DC: Defense Science Board, February 2017. <http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>.
- Miller, James N., Jr., and Richard Fontaine. *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict*. Washington, DC: CNAS, September 2017. <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Project Pathways-Finalb.pdf?mtime=20170918101505>.
- Miller, Rich. "Con Edison Shuts off Power in Lower Manhattan." *DataCenter Knowledge*, October 29, 2012. <http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutdown>.
- MISO (Midcontinent Independent System Operator). *Geomagnetic Disturbance Operations Plan*. SO-P-AOP-01 Rev: 1. Carmel, IN: MISO, June 9, 2017. [https://old.misoenergy.org/\\_layouts/miso/ecm/redirect.aspx?id=252214](https://old.misoenergy.org/_layouts/miso/ecm/redirect.aspx?id=252214).
- . "MISO January 17–18 Maximum Generation Event Overview." Slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018. <https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf>.
- Mitchell, A. Weiss. "The Case for Deterrence by Denial." *American Interest*, August 12, 2015. <https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/>.
- "M-1 Reserve Margin." NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.
- Murauskaite, Egle. "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment." *38 North*, September 12, 2014. <http://www.38north.org/2014/09/emurauskaite091214/>.
- Nakashima, Ellen. "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks." *Washington Post*, July 8, 2017. [https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47\\_story.html](https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html).
- NARUC (National Association of Regulatory Utility Commissioners). *Cybersecurity: A Primer for State Utility Regulators*. Version 3.0. Washington, DC: NARUC, January 2017. <https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F>.

- . *Resolution on Physical Security*. Washington, DC: NARUC, July 16, 2014. <https://pubs.naruc.org/pub.cfm?id=53A0CAA5-2354-D714-5127-E0C411BAD460>.
- NASEO (National Association of State Energy Officials). “Comments of the National Association of State Energy Officials.” In *Response to RIN 1901–AB40*. [https://www.naseo.org/Data/Sites/1/naseo-comments\\_rin-1901%E2%80%93ab40.pdf](https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901%E2%80%93ab40.pdf).
- NATF (North American Transmission Forum). *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—A Spare Tire Approach*. Charlotte, NC: NATF, 2017. <http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf>.
- . *North American Transmission Forum External Newsletter*. Charlotte, NC: NATF, January 2018. <https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf>.
- National Defense Authorization Act for Fiscal Year 2017. Public Law 114-328. *U.S. Statutes at Large* 130 (2016): 2685–2687. <https://www.gpo.gov/fdsys/pkg/PLAW-114publ328/pdf/PLAW-114publ328.pdf>.
- NERC (North American Electric Reliability Corporation). *BAL-002-2(i)—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. Washington, DC: NERC, January 1, 2018. [https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2\(i\).pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2(i).pdf).
- . *CIP-014-2—Physical Security*. Washington, DC: NERC, October 2, 2015. <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.
- . *EOP-010-1—Geomagnetic Disturbance Operations*. Washington, DC: NERC, June 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States).
- . *EOP-011-1—Emergency Operations*. Washington, DC: NERC, April 1, 2017. [https://www.nerc.com/\\_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).
- . *Glossary of Terms Used in NERC Reliability Standards*. Washington, DC: NERC, last updated July 3, 2018. [https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary\\_of\\_Terms.pdf](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf).
- . *Grid Security Exercise: GridEx III Report*. Atlanta, GA: NERC, March 2016. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.
- . *Grid Security Exercise GridEx IV: Lessons Learned*. Atlanta, GA: NERC, March 28, 2018. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf>.
- . *History of NERC*. Washington, DC: NERC, August 2013. <http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf>.
- . *Hurricane Harvey Event Analysis Report*. Washington, DC: NERC, March 2018. [https://www.nerc.com/pa/rrm/ea/Hurricane\\_Harvey\\_EAR\\_DL/NERC\\_Hurricane\\_Harvey\\_EAR\\_20180309.pdf](https://www.nerc.com/pa/rrm/ea/Hurricane_Harvey_EAR_DL/NERC_Hurricane_Harvey_EAR_20180309.pdf).



- . “Informational Filing on the Definition of ‘Adequate Level of Reliability.’” Filing to the Federal Energy Regulatory Commission. May 10, 2013. [https://www.nerc.com/pa/Stand/Resources/Documents/Adequate\\_Level\\_of\\_Reliability\\_Definition\\_\(Informational\\_Filing\).pdf](https://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf).
- . *IRO-008-2—Reliability Coordinator Operational Analysis and Real-Time Assessments*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/IRO-008-2.pdf>.
- . *PRC-010-2—Under Voltage Load Shedding*. Washington, DC: NERC, April 2, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States).
- . *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*. Atlanta, GA: NERC, December 13, 2017. [https://www.nerc.com/comm/OC\\_Reliability\\_Guidelines\\_DL/Gas\\_and\\_Electrical\\_Operational\\_Coordination\\_Considerations\\_20171213.pdf](https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Gas_and_Electrical_Operational_Coordination_Considerations_20171213.pdf).
- . *Reliability Terminology*. Atlanta, GA: NERC, August 2013. <https://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf>.
- . *Short-Term Special Assessment: Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation*. Atlanta, GA: NERC, May 2016. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric\\_Final.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric_Final.pdf).
- . *Standard PRC-006-3—Automatic Underfrequency Load Shedding*. Washington, DC: NERC, October 1, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States).
- . *Technical Report Supporting Definition of Adequate Level of Reliability*. Washington, DC: NERC, March 26, 2013. <https://www.nerc.com/comm/Other/Pages/Adequate%20Level%20of%20Reliability%20Task%20Force%20ALRTF.aspx>.
- . *TOP-001-3—Transmission Operations*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-001-3.pdf>.
- . *TPL-007-1—Transmission System Planned Performance for Geomagnetic Disturbance Events*. Washington, DC: NERC, December 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States).
- . *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power Phase II: A Vulnerability and Scenario Assessment for the North American Bulk Power System*. Atlanta, GA: NERC, May 2013. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC\\_PhaseII\\_FINAL.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf).
- . *2016 Long-Term Reliability Assessment*. Atlanta, GA: NERC, December 2016. <https://www.nerc.com/pa/rapa/ra/reliability%20assessments%20dl/2016%20long-term%20reliability%20assessment.pdf>.
- . *VAR-001-4.2—Voltage and Reactive Control*. Washington, DC: NERC, September 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/VAR-001-4.2.pdf>.



- NERC (North American Electric Reliability Corporation) Steering Group. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* Princeton, NJ: NERC, July 13, 2014. [https://www.nerc.com/docs/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](https://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC (North American Electric Reliability Corporation) System Protection and Control Subcommittee. *Reliability Fundamentals of System Protection*. Princeton, NJ: NERC, December 2010. [https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals\\_Approved\\_20101208.pdf](https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals_Approved_20101208.pdf).
- NETL (National Energy Technology Laboratory). *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units—Volume I: The Critical Role of Thermal Units during Extreme Weather Events*. Washington, DC: DOE, March 13, 2018. <https://www.netl.doe.gov/research/energy-analysis/search-publications/vuedetails?id=2594>.
- Newman, Lily Hay. “Hacker Lexicon: What Is the Attribution Problem?” *Wired*, December 24, 2016. <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.
- NIAC (National Infrastructure Advisory Council). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. Washington, DC: NIAC, August 2017. <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>.
- Nielsen, Kirstjen M. “National Cybersecurity Summit Keynote Speech.” DHS (Department of Homeland Security). Released July 31, 2018. <https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech>.
- “NOAA Space Weather Scales.” NOAA. April 2011. <https://www.swpc.noaa.gov/sites/default/files/images/NOAAscales.pdf>.
- “North America.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/Canada.aspx>.
- “The North Atlantic Treaty.” North Atlantic Treaty Organization. April 4, 1949 (as amended). [https://www.nato.int/cps/ic/natohq/official\\_texts\\_17120.htm](https://www.nato.int/cps/ic/natohq/official_texts_17120.htm).
- Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016/2017): 44–71. [https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\\_a\\_00266](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266).
- Obama, Barack. *Executive Order—Assignment of National Security and Emergency Preparedness Communications Functions*. Washington, DC: The White House, July 6, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness->.
- . *Executive Order—Coordinating Efforts to Prepare the Nation for Space Weather Events*. Washington, DC: The White House, October 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events>.
- . *Executive Order—Improving Critical Infrastructure Cybersecurity*. Executive Order 13636. Washington, DC: The White House, February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

- . *Executive Order—National Defense Resources Preparedness*. Washington, DC: The White House, March 16, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/03/16/executive-order-national-defense-resources-preparedness>.
- . *United States Cyber Incident Coordination*. Presidential Policy Directive 41. Washington, DC: The White House, July 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
- ODNI (Office of the Director of National Intelligence). *A Common Threat Framework: A Foundation for Communication*. McLean, VA: ODNI, January 26, 2018.
- Orenstein, Daniel G., and Lexi C. White. *Emergency Declaration Authorities across All States and D.C.* Edina, MN: Network for Public Health Law, June 16, 2015. [https://www.networkforphl.org/\\_asset/gxrdwm/Emergency-Declaration-Authorities.pdf](https://www.networkforphl.org/_asset/gxrdwm/Emergency-Declaration-Authorities.pdf).
- Paradise, Theodore J., et al. “ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance—RIN 1901–AB40.” Email to Jeffrey Baumgartner, US Department of Energy, February 6, 2017. [http://www.isorto.org/Documents/Report/20170206\\_Final\\_IRC-DOE\\_NOPR\\_Comments\\_re\\_Grid\\_Security\\_Emergency.pdf](http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf).
- Parfomak, Paul W. *Pipelines: Securing the Veins of the American Economy, Testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*. Washington, DC: Congressional Research Service, April 19, 2016. <http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf>.
- Parfomak, Paul W., Richard J. Campbell, Robert Pirog, Michael Ratner, Phillip Brown, John Frittelli, and Marc Humphries. *Cross-Border Energy Trade in North America: Present and Potential*. Washington, DC: Congressional Research Service, January 30, 2017. <https://fas.org/sgp/crs/misc/R44747.pdf>.
- Perry, Richard (US secretary of energy). Letter to the Federal Energy Regulatory Commission. September 28, 2017. <https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf>.
- Phillips, Tony. “Solar Shield—Protecting the North American Power Grid.” *NASA Science*, October 26, 2010. [https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\\_solarshield](https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield).
- PJM. “Comments and Responses of PJM Interconnection, L.L.C.” In *Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000). March 9, 2018. <http://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx>.
- . “Conservative Operations.” Training materials presented on January 27, 2015. <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.
- . *PJM Manual 13: Emergency Operations*. Rev. 65. Audubon, PA: PJM, January 1, 2018. <http://www.pjm.com/~/-/media/documents/manuals/m13.ashx>.

- Puryear, Cotton. "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade." *National Guard*, September 19, 2017. <http://www.nationalguard.mil/News/Article/1315685/91st-cyber-brigade-activated-as-army-national-guards-first-cyber-brigade/>.
- Reagan, Ronald. "The President's News Conference." August 12, 1986. Transcript. The American Presidency Project, Gerhard Peters and John T. Woolley. <http://www.presidency.ucsb.edu/ws/?pid=37733>.
- "Reliability Coordinators." NERC (North American Electric Reliability Corporation). As of June 1, 2015. <https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.
- "REMEDYS: Research Exploring Malware in Energy Delivery Systems." Cyber Resilient Energy Delivery Consortium. March 26, 2018. <https://cred-c.org/researchactivity/remedys-research-exploring-malware-energy-delivery-systems>.
- "The Role of Microgrids in Helping to Advance the Nation's Energy System." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/role-microgrids-helping>.
- "Roles and Responsibilities of Governments in Natural Resources." Natural Resources Canada. Last modified October 2, 2017. <http://www.nrcan.gc.ca/mining-materials/taxation/8882>.
- Rosenbach, Eric. "Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks." *Prepared Statement for the United States Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*. June 12, 2017. [https://www.foreign.senate.gov/imo/media/doc/061317\\_Rosenbach\\_Testimony.pdf](https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf).
- "Sandia's Grid Modernization Program Newsletter." Sandia National Laboratories. December 2017. <https://content.govdelivery.com/accounts/USDOESNLEC/bulletins/1c11ce6>.
- Schwartz, Ian. "Sen. Tillis: We Are Living in a Glass House Throwing Rocks Complaining about Election Interference." *RealClear Politics*, January 5, 2017. [https://www.realclearpolitics.com/video/2017/01/05/sen\\_tillis\\_we\\_are\\_living\\_in\\_a\\_glass\\_house\\_throwing\\_rocks\\_complaining\\_about\\_election\\_interference.html](https://www.realclearpolitics.com/video/2017/01/05/sen_tillis_we_are_living_in_a_glass_house_throwing_rocks_complaining_about_election_interference.html).
- "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response." DOE (Department of Energy). February 14, 2018. <https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency>.
- SERC. *Conservative Operations Guidelines*. Guide-800-101. Charlotte, NC: SERC, May 20, 2015. [https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines\\_rev-0-\(05-20-15\).pdf?sfvrsn=2](https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2).
- Severe Impact Resilience Task Force. *Severe Impact Resilience: Considerations and Recommendations*. Washington, DC: NERC, May 9, 2012. [https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF\\_Final\\_May\\_9\\_2012-Board\\_Accepted.pdf](https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf).

- Shelton, William L. "Threats to Space Assets and Implications for Homeland Security." *Written Testimony before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*. March 29, 2017. <http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf>.
- Sistrunk, Chris. "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)." *SANS Industrial Control Systems Security Blog*, January 8, 2016. <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>.
- Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (Winter 2016/17): 73–109. [https://www.mitpressjournals.org/doi/10.1162/ISEC\\_a\\_00267](https://www.mitpressjournals.org/doi/10.1162/ISEC_a_00267).
- Smith, Rebecca. "U.S. Officials Push New Penalties for Hackers of Electrical Grid." *Wall Street Journal*, August 5, 2018. <https://www.wsj.com/articles/u-s-officials-push-new-penalties-for-hackers-of-electrical-grid-1533492714>.
- Smith, Scott S. "Roles and Responsibilities for Defending the Nation from Cyber Attack." *Testimony Before the Senate Armed Services Committee*. October 19, 2017. <https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities>.
- Sobczak, Blake, Hannah Northey, and Peter Behr. "Cyber Raises Threat against America's Energy Backbone." *Energy Wire*, May 23, 2017. <https://www.eenews.net/stories/1060054924/>.
- Social Media Working Group for Emergency Services and Disaster Management. *Countering False Information on Social Media in Disasters and Emergencies*. Washington, DC: DHS, March 2018. [https://www.dhs.gov/sites/default/files/publications/SMWG\\_Countering-False-Info-Social-Media-Disasters-Emergencies\\_Mar2018-508.pdf](https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf).
- "Spare Transformers." EEI (Edison Electric Institute). n.d. <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.
- Stanley, Andrew J. *Mapping the U.S.-Canada Energy Relationship*. Washington, DC: CSIS, May 2018. [https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507\\_Stanley\\_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507_Stanley_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz).
- "State and Local Energy Assurance Planning." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/energy-assurance/emergency-preparedness/state-and-local-energy-assurance-planning>.
- State of New Jersey Board of Public Utilities. *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196). March 18, 2016. <http://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf>.
- Stockton, Paul. On behalf of Exelon Corporation. *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*. Docket No. RM18-1-000. October 23, 2017.
- . "Thresholds and Criteria for Declaring Grid Security Emergencies." Study for the US Department of Energy. January 31, 2018.



- Sukumar, Arun M. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare* (blog), July 4, 2017. <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.
- "Transmission Equipment Ready When Needed." Grid Assurance. n.d. <http://www.gridassurance.com/equipment-subscribers/>.
- Trump, Donald. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Executive Order 13800. Washington, DC: The White House, May 11, 2017. <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
- Ucci, Daniele, Leonardo Aniello, and Roberto Baldoni. "Survey on the Usage of Machine Learning Techniques for Malware Analysis." *ACM Transactions on the Web* 1, no. 1 (October 2017): 1:1–1:34. <https://pdfs.semanticscholar.org/d310/47e426b8b5c2aa52108899a800bedd966f07.pdf>.
- "United States Mandatory Standards Subject to Enforcement." NERC. n.d. <https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States>.
- U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington, DC: DOE, April 2004. <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.
- US Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington, DC: US Cyber Command, released March 2018. <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>.
- Van Broekhoven, S. B., N. Judson, S. V. T. Nguyen, and W. D. Ross. *Microgrid Study: Energy Security for DoD Installations*. Technical Report 1164. Lexington, MA: MIT, June 2012. <https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf>.
- Vine, Doug. *Interconnected: Canadian and U.S. Electricity*. Arlington, VA: Center for Climate and Energy Solutions, March 2017. <https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf>.
- Walker, Bruce J. *Written Testimony before the U.S. Senate Committee on Energy and Natural Resources*. March 1, 2018. [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=1C574731-A9C0-4E1C-9E05-15C492E332B1](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1).
- Weiss, Walter. "Rapid Attack Detection, Isolation and Characterization Systems (RADICS)." Defense Advanced Research Projects Agency. n.d. <https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems>.
- Western Electricity Coordinating Council. "Conservative System Operations." Training slides. n.d. <http://docplayer.net/55224883-Conservative-system-operations.html>.
- The White House. *National Security Strategy of the United States of America*. Washington, DC: The White House, December 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- "Work Continues on ITC Lake Erie Project." *Transmission Hub*, February 19, 2018. <https://www.transmissionhub.com/articles/2018/02/work-continues-on-itc-lake-erie-project.html>.





## Acknowledgments

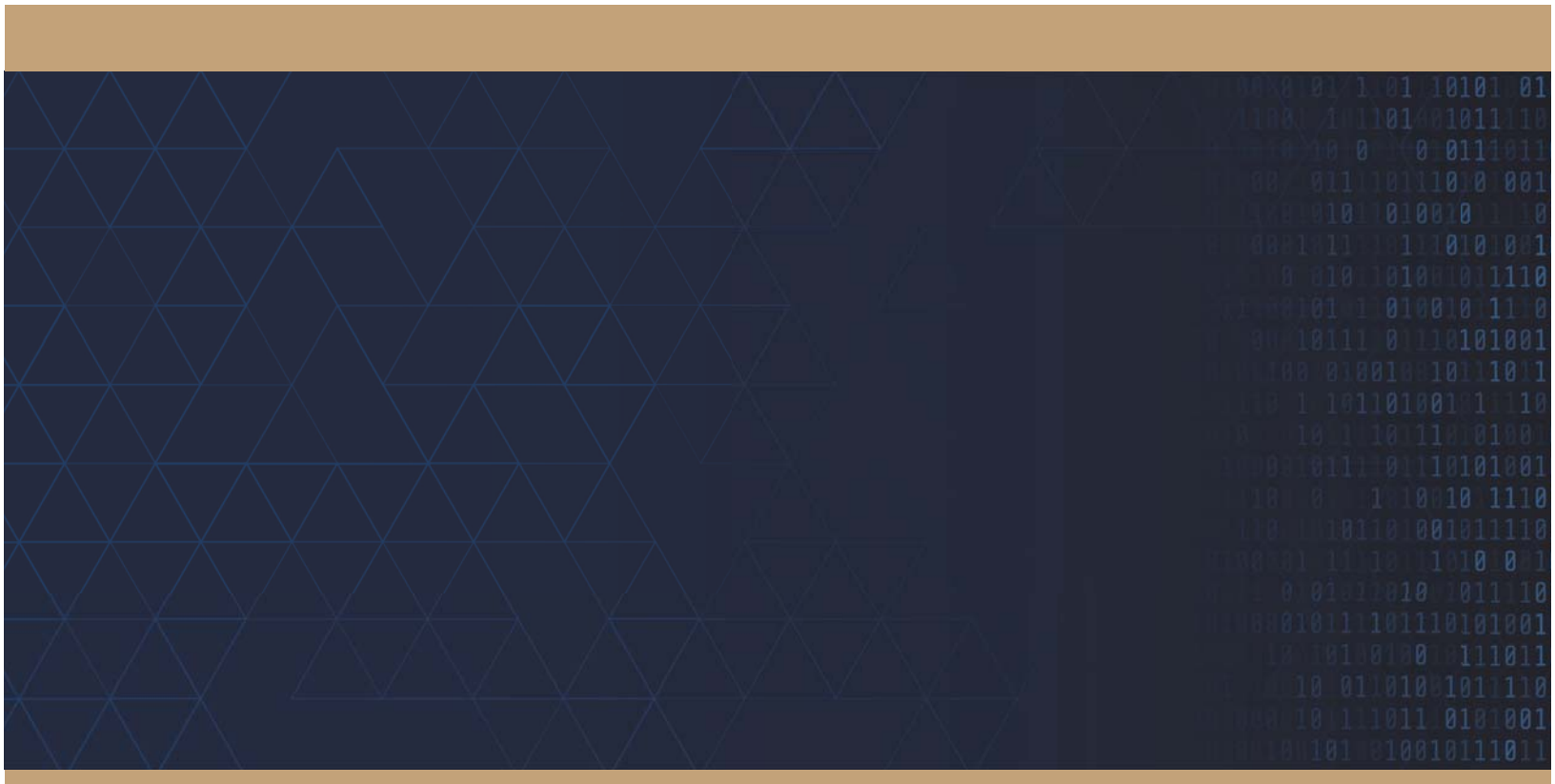
My special thanks go to Robert Denaburg, senior analyst at Sonecon LLC. I also thank the following colleagues for helpful reviews of this study: Michael Assante (SANS Institute); Wayne Austad (Idaho National Laboratory); Terry Boston; Stuart Brindley; Gerry Cauley; Richard Danzig (JHU/APL); Daniel Elmore (Idaho National Laboratory); Peter Grandgeorge (Berkshire Hathaway Energy); Emily Goldman (US Cyber Command); Sean Griffin (ecubed us LLC); Dave Halla (JHU/APL); Jon Jipping (ITC Holdings); Debra Lavoy (Narrative Builders); Bill Lawrence (NERC); Joseph Maurio (JHU/APL); James Miller (JHU/APL); Michael Moskowitz (JHU/APL); Richard Mroz; Steven T. Naumann (Exelon Corporation); Catherine Peacock (JHU/APL); Emilia Probasco (JHU/APL); Erin Richardson (JHU/APL); David Roop (Dominion Energy); Matthew Schaffer (JHU/APL); senior leaders at Southern Company; Kyle Thomas (Dominion Virginia Power); and Virginia Wright (Idaho National Laboratory). I also thank the many additional industry and government reviewers who preferred to remain anonymous.

## About the Author

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC, and a senior fellow of JHU/APL. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support in Superstorm Sandy and other disasters. Dr. Stockton also served as the Department of Defense (DOD) domestic crisis manager and was responsible for defense critical infrastructure protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors and was responsible for developing and overseeing the implementation of DOD security policy in the Western Hemisphere. Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation, associate provost of the Naval Postgraduate School, and director of the school's Center for Homeland Defense and Security. Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the author of *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System* (Laurel, MD: JHU/APL, 2016) and numerous other publications. He served as the facilitator of the GridEx IV exercise (November 2017) and is a member of the Homeland Security Advisory Council and other public and private sector boards.









**To:** Joe McClelland

**Through:** (b) (6), David Andrejcak, Harry Tom

**From:** (b) (6)

**Subject:** Summary of “Enhancing the Resilience of the Nation’s Electricity System”

**Date:** March 20, 2018

**I. Introduction**

(b) (5)

[Redacted text block]

(b) (5)

**II. Summary of Study Report**

(b) (5)

[Redacted text block]

[Redacted text block]

[Redacted text block]

---

<sup>1</sup> Available at <http://nap.edu/24836>

(b) (5)



(b) (5)

A large rectangular area of the document is completely redacted with a solid black box. The redaction covers approximately the top third of the page content.A large rectangular area of the document is completely redacted with a solid black box. This redaction covers the middle section of the page, below the first redacted block.A large rectangular area of the document is completely redacted with a solid black box. This redaction covers the bottom section of the page, below the second redacted block.

(103). Recommendation 5.5 is for the DOE and DHS to “evaluate and recommend the  
(b) (5)

[Redacted]

[Redacted]

[Redacted]

(b) (5)



(b) (5) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

(b) (5) [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (5) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

**From:** [Andrew Dodge](#)  
**To:** (b) (6)  
**Subject:** FW: Resilience Report  
**Date:** Tuesday, April 10, 2018 8:30:53 AM  
**Attachments:** [NAP resilience summary.docx](#)  
[Enhancing the Resilience of the Nations Electricity System.pdf](#)

---

fyi

---

**From:** (b) (6)  
**Sent:** Thursday, March 22, 2018 10:36 AM  
**To:** Harry Tom <Harry.Tom@ferc.gov>; (b) (6) David Andrejczak  
<David.Andrejczak@ferc.gov>  
**Cc:** Andrew Dodge <Andrew.Dodge@ferc.gov>  
**Subject:** Resilience Report

Harry, (b) (6), and Dave,

Attached is a requested draft summary of the National Academies report on Resilience. I've added Dave A to this distribution and cc'd Andy for his information.

I've attached a PDF of the report. I have Joe's hard copy – I can return it via Rose.

(b) (6)  
Federal Energy Regulatory Commission  
Office of Energy Infrastructure Security  
(b) (6)

# RESILIENCE FOR **GRID SECURITY** EMERGENCIES

**Opportunities for Industry–Government Collaboration**

**National Security Perspective**



Paul N. Stockton

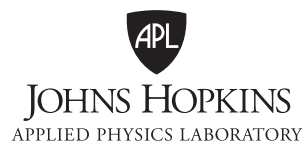




# **RESILIENCE FOR GRID SECURITY EMERGENCIES**

Opportunities for Industry–Government Collaboration

Paul N. Stockton



Copyright © 2018 The Johns Hopkins University Applied Physics Laboratory LLC. All Rights Reserved.

This National Security Perspective contains the best opinion of the author at time of issue. The views expressed in this study are solely those of the author and do not necessarily reflect the opinions, practices, policies, procedures, or recommendations of the US Department of Energy or any other US government agency or of JHU/APL sponsors.

## Contents

Figures.....	v
Summary .....	vii
<b>Developing Emergency Orders under the FPA.....</b>	<b>1</b>
Drafting Template Emergency Orders before Attacks Occur .....	3
Participants in Drafting and Implementing Emergency Orders .....	5
Goals and Specific Design Requirements for Developing Emergency Orders .....	11
<b>Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies .....</b>	<b>13</b>
Threats That Can Trigger Grid Security Emergencies .....	13
Thresholds for Declaring Grid Security Emergencies .....	17
Data Sharing and Consultations with Industry .....	25
<b>Grid Security Emergency Phases and Order Design Options .....</b>	<b>28</b>
Preattack Options.....	29
Extraordinary Measures when Attacks Are Occurring.....	33
Emergency Orders to Support Power Restoration.....	35
<b>Additional Emergency Order Design Parameters and Supporting Initiatives .....</b>	<b>38</b>
Deterring and Defeating US Adversaries.....	38
Communications Requirements for Issuing and Employing Emergency Orders .....	46
The Deeper Value Proposition for Emergency Orders.....	52
<b>Conclusions and Recommendations for Broader Progress .....</b>	<b>58</b>
Employing Additional Emergency Authorities for Cross-Sector Resilience.....	59
Extended Partnership Requirements within the United States and Abroad.....	64
Playing Defense in Cyberwarfare .....	70
Bibliography .....	75
Acknowledgments.....	93
About the Author .....	93





Figures

Figure S-1. Grid Security Emergency Phases..... viii

Figure 1. Stakeholders for Building Grid Security Emergency Resilience.....10

Figure 2. ODNI Cyber Threat Framework.....20

Figure 3. Elements of the Cyber Incident Severity Schema .....21

Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies.....26

Figure 5. Emergency Order Matrix: Examples of Order Designs .....29

Figure 6. Categories for Protecting Defense Critical Electric Infrastructure .....41

Figure 7. NERC Regional Entities across North America .....67

Figure credits:

Figure 2: “The Cyber Threat Framework,” ODNI (Office of the Director of National Intelligence), n.d., <https://www.dni.gov/index.php/cyber-threat-framework>.

Figure 3: DHS (US Department of Homeland Security), *National Cyber Incident Response Plan* (Washington, DC: DHS, December 2016).

Figure 7: Information from NERC (North American Electric Reliability Corporation), <http://www.nerc.com/Pages/default.aspx>; figure reprinted from Susan Lee, Michael Moskowitz, and Jane Pinelis, *Quantifying Improbability: An Analysis of the Lloyd’s of London Business Blackout Cyber Attack Scenario*, National Security Report NSAD-R-18-027 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018).



## Summary

The US Congress has opened the door to novel strategies for defending the country's electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act (FPA) in December 2015, Congress granted the secretary of energy vast new authorities to use when the president declares a grid security emergency. Most important, the secretary can issue emergency orders to power companies to protect and restore grid reliability when attacks on their systems are "imminent" or under way.<sup>1</sup> The FPA is silent, however, on what the secretary might require companies to do and how such orders can bolster their emergency operations.

The onset of an attack would be the worst possible time to develop emergency orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid. They could then adjust such orders to fit the specific circumstances of an attack. Developing emergency orders in advance would also help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. Companies could then exercise their contingency plans to build preparedness for response operations and contribute to national security in unprecedented ways.

This report is structured to help the electricity subsector and Department of Energy (DOE) develop emergency orders to defend the grid against potentially catastrophic cyber and physical attacks. The report highlights the phases that grid security emergencies are likely to entail. It analyzes the requirements that emergency orders will need to meet for each phase, and how orders can supplement existing utility plans and capabilities to fill gaps in grid resilience. The report also examines how emergency orders can strengthen deterrence against grid attacks and help defeat adversaries if deterrence fails.

The president must declare a grid security emergency before the secretary of energy can issue emergency orders. However, the FPA offers only broad and potentially ambiguous criteria for making that determination, especially for attacks that are imminent. Such ambiguity is useful; the president should retain the flexibility to declare grid security emergencies in a wide range of circumstances. Nevertheless, policy makers may find it useful to establish more detailed criteria to support their internal deliberations. This report proposes options for them to consider, including criteria derived from the electric industry's requirements to preserve "adequate levels of reliability" against cascading blackouts and other multistate grid disruptions. The report also examines how industry and government agencies can refine their information sharing mechanisms to support the emergency declaration process.

Once the president makes such a declaration, grid security emergencies may roll out in three phases, each of which provides the basis for developing a distinct set of template emergency orders. Figure S-1 illustrates these phases. The first will occur if the president determines that an attack is imminent. A well-established basis already exists for developing preattack emergency orders. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions. Such operations might include staffing up emergency operations centers, prepositioning recovery personnel and supplies, increasing available generation to help manage grid instabilities, and taking other precautionary measures. A key advantage of many of these options is that utilities can carry them

---

<sup>1</sup> Fixing America's Surface Transportation Act, Public Law 114-94.

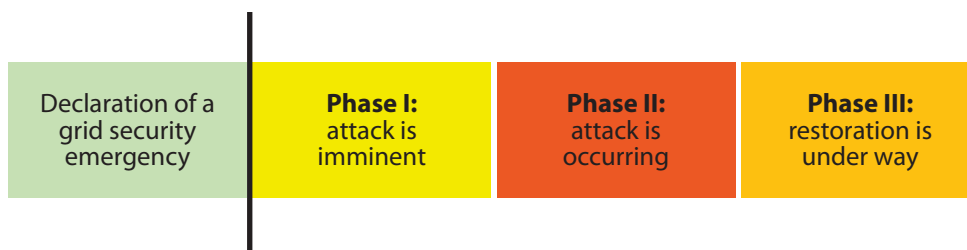


Figure S-1. Grid Security Emergency Phases

out without disrupting normal service; if the hurricane veers back to sea, utilities will have no regrets about having implemented them.

Power companies should help DOE develop equivalent “no-regrets” conservative operations to protect the grid against imminent cyber and physical attacks. A growing number of utilities are already adapting their existing plans for conservative operations to counter physical and cyber risks. These initiatives provide a strong foundation for developing emergency orders that will leverage best practices and help ensure that utilities will implement them on a consistent, nationwide basis. Moreover, because many of these conservative operations will inflict little or no disruption on normal grid service, they are ideal for protecting the grid when attacks are increasingly probable but not certain to occur. DOE and industry should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The next phase of grid security emergencies will occur when attacks are under way. Emergency orders for this phase can help utilities prevent power failures from cascading across the United States and prioritize the sustainment of electric service for military bases and facilities essential for public health (e.g., major regional hospitals and metropolitan water systems). As with conservative operations, existing electric industry plans and capabilities provide a strong basis for developing such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Orders for equivalent *extraordinary measures* could provide useful arrows in the quiver in grid security emergencies.

The final phase of grid security emergencies will commence as utilities begin restoring service to areas without power. Attacks that damage or destroy large numbers of high-voltage transformers and other difficult-to-replace grid components could create outages that darken major portions of the United States for many weeks, or even months. Power companies and DOE already have initiatives under way to meet this challenge. They should also collaborate to develop emergency orders to *support restoration*, which could facilitate the movement of replacement transformers and assist utilities in other strategically vital ways.

These grid security emergency phases could overlap. In particular, once power companies begin restoring power, adversaries may launch follow-on attacks that necessitate continued load shedding and other extraordinary measures to protect grid reliability. At the outset of an emergency, utilities should prepare to receive and implement orders across all emergency phases in an integrated way.

DOE and its industry partners should also design emergency orders to fill underlying gaps in preparedness for cyber and physical attacks. Power companies already have extensive plans and capabilities to protect and restore grid reliability against these threats, in part because mandatory reliability standards require them to do so. Grid owners and operators are also spring-loaded to employ emergency measures the moment they are

needed. Indeed, the North American Reliability Corporation can fine most major US power companies if they fail to implement emergency actions to protect grid reliability.<sup>2</sup> This robust industry preparedness begs the question: what added value can DOE emergency orders provide?

The most obvious benefit lies in the FPA's provisions for regulatory waivers and cost recovery. When grid owners and operators carry out emergency orders, they may have to violate environmental standards and other regulatory requirements. The FPA now protects entities from being punished for such violations if they occur while complying with emergency orders. The act also provides for the recovery of costs that companies will incur in implementing emergency orders. This report examines how further waiver and cost-recovery measures could reinforce preparedness for grid security emergencies.

Emergency orders can also help support national security in new and far-reaching ways. Russia, China, and other potential adversaries will not strike the grid simply to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to US defense installations responsible for deploying forces to the region, as well as to ports and other civilian infrastructure that supports force projection. Emergency orders can be designed to help deter—and, if necessary, defeat—such attacks. This report proposes specific options to do so, in support of the *National Security Strategy of the United States of America* and other sources of US policy guidance.

Some of these options will require harsh and politically contentious decisions on allocating power if adversaries severely disrupt the grid. Emergency orders for prioritized load shedding provide a case in point. To help deter attacks, grid owners and operators need the ability to sustain service to critical defense installations, including those responsible for conducting response operations against (and imposing costs on) potential attackers for however long a conflict may last. The ability to protect power flows to hospitals and other facilities vital for public health and safety will be valuable as well. However, if adversaries disrupt sufficient grid generation and transmission assets, sustaining reliable service to these installations may require utilities to curtail service to other customers. Government officials—and, ultimately, the president—should make such decisions and provide political top cover and liability protections for power companies that implement them.

Grid security emergencies will also create unprecedented challenges for government and industry to communicate with the American people. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Against a backdrop of fear and uncertainty, adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks. Adversaries may also disrupt the phone and internet-based communications systems utilities typically use to coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications playbooks to prepare for grid security emergencies, and they should make doing so a core component of the emergency order development process.

DOE and its industry and government partners will need to conduct intensive follow-on work to finalize the development of emergency orders and build utility-specific contingency plans to implement the orders in ways that account for accelerating structural changes in the electricity subsector. Their collaborative efforts will

---

<sup>2</sup> Bulk power system entities, including generation and high-voltage transmission companies, are subject to NERC's mandatory reliability standards and emergency orders under the FPA. For an analysis of applicability issues, see pages 5–10.



require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, as utilities and DOE tackle the immediate challenges of developing emergency orders, they should also explore broader opportunities to build preparedness for grid security emergencies. One such opportunity lies in integrating the use of emergency orders with other federal authorities. The secretary of energy can issue grid security emergency orders only to power companies. Increasingly, however, power generation depends on the flow of natural gas. Communications systems and other infrastructure sectors will also play critical roles in supporting power restoration. The secretary of energy and other federal leaders have additional authorities beyond section 215A of the FPA that can strengthen cross-sector resilience for grid security emergencies. However, achieving these benefits will require private and public sector leaders to preplan and exercise the coordinated use of these authorities, and to develop “whole-of-government” strategies to support infrastructure owners and operators.

Coordination with Canada could be valuable as well. The electric grids of the United States and Canada are deeply interconnected, and adversary-induced failures in one nation may rapidly cascade into the other. The secretary of energy does not have the authority to issue emergency orders to power companies in Canada (or in any other nation). Yet, significant opportunities exist to build on current reliability protections and emergency coordination mechanisms between US and Canadian utilities. The United States could also develop collaborative plans with Mexico as well as US allies in Europe and Asia.

In addition, DOE and its partners should explore further opportunities to help deter cyber attacks and defeat US adversaries if deterrence fails. The US *National Security Strategy* emphasizes that the United States needs to convince adversaries not only that they will suffer costly consequences if they attack but also that attacking will not accomplish the objectives they seek—in other words, achieve deterrence by denial. Yet, leading scholars of deterrence argue that deterrence by denial will be extraordinarily difficult to establish in cyberspace. Emergency orders and implementation plans can help meet these challenges by strengthening grid resilience in novel ways. Government agencies should also consider developing broader doctrine to “play defense” if cyberwarfare breaks out, and coordinate grid security emergency operations at home with measures to suppress adversary attacks at their source.

The foundational importance of the electric grid makes it a prime target for attack. As secretary of energy Richard Perry emphasizes, “America’s greatness depends on a reliable, resilient electric grid” that can power the economy, support national defense, and provide for the necessities of modern life.<sup>1</sup> To prevent adversaries from exploiting the United States’ dependence on the grid, the Department of Energy (DOE) and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter—and, if necessary, defeat—attacks on the grid.<sup>2</sup>

The FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the Fixing America’s Surface Transportation (FAST) Act amendments to the FPA, it greatly expanded the secretary of energy’s authority to issue emergency orders to grid owners and operators. Under section 215A of the act, “the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability” of critical electric infrastructure in a grid security emergency.<sup>3</sup> Before the secretary can issue those orders, the president

must first declare a grid security emergency when attacks on the grid are imminent or under way.<sup>4</sup>

However, legislators provided scant guidance on what the secretary might order power companies to do. DOE and its partners in the electricity subsector are now assessing which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats. This report supports their work by examining possible emergency orders and analyzing broader opportunities to strengthen resilience for grid security emergencies.

## Developing Emergency Orders under the FPA: Collaborative Opportunities, Fundamental Goals, and Overarching Design Requirements

The secretary of energy’s new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, “the nine most terrifying words in the English language are ‘I’m from the government and I’m here to help.’”<sup>5</sup> Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already taking steps to minimize such risks. Especially valuable, the department has incorporated industry recommendations on the process by which the secretary should issue emergency orders to utilities, and—“if practicable”—consult with industry before those orders are issued.<sup>6</sup> The next collaborative step should be to include power companies in

<sup>1</sup> Perry, letter to the FERC.

<sup>2</sup> The 2015 FAST Act amendments to the FPA provide the authority to undertake these efforts. Prior to 2015, section 202(c) of the FPA already authorized the secretary of energy to issue emergency orders to order “temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest.” That provision also specified that the secretary could exercise such powers “during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes.” See “DOE’s Use of Federal Power Act Emergency Authority,” DOE. The 2015 FAST Act amendments to the FPA gave the secretary further powers (mostly incorporated in section 215A of the act), which are the primary focus of this report.

<sup>3</sup> 16 U.S.C. § 824o, (b)(1).

<sup>4</sup> The analysis that follows examines the definition of such emergencies in the FPA and potential thresholds for declaring them.

<sup>5</sup> Reagan, “President’s News Conference.”

<sup>6</sup> DOE, “RIN 1901–AB40,” 1176; EEI, “Comments”; and Paradise et al., “ISO-RTO Council Comments.”

designing template emergency orders. Grid owners and operators have unequaled knowledge of their own infrastructure and operating procedures and extensive experience in employing emergency measures to protect and restore grid reliability.<sup>7</sup> They are well positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses—and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders would be most useful to help defend their systems and effectively supplement the emergency measures utilities would already be taking on their own. Utilities will also play a critical role in building company-specific plans to implement emergency orders, exercising those plans, and identifying remaining gaps to fill.

Strategic guidance from DOE and other government departments will be just as critical for designing emergency orders. Federal leadership will be essential to ensure that emergency orders help achieve overarching US security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing emergency orders to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.<sup>8</sup> Government officials can also shape emergency orders and supporting initiatives to help implement US cyber resilience strategies, including the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

(May 2017) and DOE's *Multiyear Plan for Energy Sector Cybersecurity* (March 2018).<sup>9</sup>

In addition, DOE will play a critical role in coordinating industry and government operations during grid security emergencies. The same congressional amendments that granted the secretary expansive new emergency authorities also specified that DOE shall be the federal government's "lead sector-specific agency for cybersecurity for the energy sector." As such, the secretary is responsible for collaborating with grid owners and operators, regulators, and other government agencies to help mitigate incidents and provide broader support to the energy sector.<sup>10</sup>

Federal incident response operational plans provide a broader framework for building these collaborative mechanisms. Presidential Policy Directive 41, *United States Cyber Incident Coordination* (July 2016), the *National Cyber Incident Response Plan* (December 2016), and the *National Response Framework* (June 2016) offer particularly useful guidance for building grid-specific coordination mechanisms.<sup>11</sup> DOE is also strengthening its own internal mechanisms and organizational structure to manage cyber incidents.<sup>12</sup> These changes further position the department to effectively collaborate with industry in developing and executing emergency orders.

<sup>9</sup> Trump, *Executive Order on Strengthening Cybersecurity*; and DOE, *Multiyear Plan*. See also Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*; and DHS, *Cybersecurity Strategy*.

<sup>10</sup> Fixing America's Surface Transportation Act, Public Law 114-94, 1779 (hereafter cited as FAST Act).

<sup>11</sup> Obama, *United States Cyber Incident Coordination*; DHS, *National Cyber Incident Response Plan*; and DHS, *National Response Framework*.

<sup>12</sup> DOE, *Multiyear Plan*, 28. DOE has also established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to "enable more coordinated preparedness and response to natural and man-made threats." See "Secretary of Energy Forms New Office," DOE.

<sup>7</sup> FERC and NERC, *Restoration and Recovery Plans*; FERC and NERC, *Planning Restoration Absent SCADA or EMS (PRASE)*; and FERC and NERC, *Recommended Study: Blackstart Resources Availability (BRAv)*. Additional BPS plans, exercises, and mandatory reliability standards are addressed in subsequent portions of the report.

<sup>8</sup> White House, *National Security Strategy*.

## Drafting Template Emergency Orders before Attacks Occur

The FPA specifies that before issuing emergency orders “the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action,” consult with appropriate power companies and other grid resilience stakeholders.<sup>13</sup> But opportunities for such consultations may be sharply limited. Adversaries may strike the grid with little or no warning. Moreover, when attacks are imminent or under way, rapidly issuing emergency orders may be crucial to help prevent cascading failures and other widespread disruptions. This imperative for speed could make consultations impractical.

To enable collaboration and minimize the risk that DOE will have to create orders amid the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, assistant secretary of energy for electricity delivery and energy reliability, stated in March 2018: “In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.”<sup>14</sup> Power companies and other electricity subsector organizations have also emphasized the need for industry and the government to jointly develop orders before adversaries strike.<sup>15</sup>

Such collaborative efforts should initially focus on creating *template orders*: orders that lay out the

basic types of actions that the secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act amendments’ potential value for the secretary to issue general orders to “protect and restore the reliability of the grid.” Vague, overly broad directives cannot provide an adequate basis for utilities to develop system-specific plans to implement them. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for “maximum generation” and increased reserve margins to more aggressive, far-reaching measures.<sup>16</sup> A key objective for such development efforts: provide a menu of agreed-upon options from which the secretary can choose as circumstances require, supported as much as possible by consultations with industry.

Developing emergency orders before attacks occur can help ensure that, as a minimalist goal, such orders will “do no harm.” By participating in the order design process, power companies can shape orders to account for system-specific engineering constraints and requirements for emergency operations. This industry input will be especially important because DOE has the authority to punish utilities for failing to comply with emergency orders, even if they are poorly designed. DOE’s grid security emergency rule specifies that “in accordance with available enforcement authorities, the secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order.”<sup>17</sup> If

<sup>13</sup> This includes the North American Electric Reliability Corporation (NERC) and its Electricity Information Sharing and Analysis Center (E-ISAC). 16 U.S.C. § 824o–1. See also the notice of proposed rulemaking and request for comment (DOE, “RIN 1901–AB40”).

<sup>14</sup> Walker, *Written Testimony*.

<sup>15</sup> See Joint Commenters, “Comments; and NASEO, “Comments.”

<sup>16</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual* 13, 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help “maintain reliable operation while meeting . . . unexpected outages of existing capacity.” See “M-1 Reserve Margin,” NERC.

<sup>17</sup> DOE, “RIN 1901–AB40,” 1182.



power companies find that an order is impossible to implement or is otherwise objectionable, they can ask DOE to reconsider it.<sup>18</sup> But adjudicating individual emergency orders amid a grid security emergency could delay time-critical actions. Instead, DOE should include industry in developing emergency orders from the start and resolve utility concerns before adversaries strike.

Preplanning to coordinate industry and government emergency operations will also be valuable. Power companies are already poised to take immediate emergency actions to protect grid reliability as circumstances require, regardless of whether the secretary issues emergency orders. It will be helpful to understand in advance how DOE can best align the issuance of such orders with industry-initiated actions. Once attacks are under way, preplanning for operational coordination will become still more important, especially if adversaries continue striking the grid and its supporting communications systems after their initial salvo.

If attacks do occur, Russia, China, or other potential adversaries will use country-specific tactics, techniques, and procedures to disrupt US infrastructure. Defending against those attacks will require tactical and operational responses that are similarly tailored to specific adversaries. Over time, it may be possible to develop (and protect adversaries from accessing) emergency orders that account for these individualized defensive requirements. US leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this report examines opportunities to do so.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders

should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high-voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military bases, regional hospitals, and other critical customers that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and identify opportunities to improve order design and execution. Training programs to prepare employees to carry out utility-specific implementation plans should also get under way as soon as possible. On a larger scale, utilities will also be able to exercise the implementation of template emergency orders within the framework of the Cyber Mutual Assistance (CMA) Program. This program enables over 140 utilities in the United States and Canada to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.<sup>19</sup> Exercises can help determine how best to align the issuance and implementation of emergency orders with these growing capabilities for mutual support.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the secretary of energy has the sole authority to issue emergency orders, the secretary may request input from senior DOE staffers

<sup>18</sup> DOE, "RIN 1901-AB40," 1181-1182.

<sup>19</sup> "ESCC's Cyber Mutual Assistance Program," ESCC.



on which orders will be most useful against specific types of attacks. The secretary may also need to brief the president and the National Security Council on proposed orders and their potential benefits. By developing orders and clarifying their respective advantages before adversaries strike, DOE and industry partners can facilitate such deliberations.

Over the longer term, industry and government leaders might structure their collaboration to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public-private and interagency coordination.<sup>20</sup> Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government-industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, to develop template emergency orders and contingency plans to implement them, power companies will need to conduct extensive operational and engineering studies and use enhanced modeling to understand the potential impact of such orders. The FAST Act amendments to the FPA provide no funding for such development efforts. Moreover, DOE and power companies are only the most obvious participants in the order design process. A wide array of other grid resilience and incident management stakeholders may also need to assist that process—including critical ones not mentioned in the FPA. Determining which specific public and private sector organizations should help shape template orders constitutes a critical first step in preparing for grid security emergencies.

## Participants in Drafting and Implementing Emergency Orders: The Bulk Power System and the Broader Electricity Subsector

An initial task in developing emergency orders will be to determine which components of the electricity subsector should participate in that effort. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>21</sup> The most obvious candidates for inclusion are the power companies that are subject to emergency orders. The FAST Act amendments to the FPA specify which components fall into that category. Chief among them are “any owner, use or operator of critical electric infrastructure or of defense critical electric infrastructure within the United States.”<sup>22</sup> The FPA also includes criteria to identify this infrastructure. Critical electric infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>23</sup> Defense critical electric infrastructure consists of grid components that serve facilities “critical to the defense of the United States” and that are vulnerable to the disruption of grid-provided power.<sup>24</sup>

However, Congress also narrowed the definition of critical electric infrastructure in a significant way. The FPA states that such infrastructure only includes assets that compose the bulk power system (BPS). BPS assets are those “facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation

<sup>20</sup> Danzig, *Catastrophic Bioterrorism*, 5–7; and Blue Ribbon Study Panel, *National Blueprint*, 13, 42–44.

<sup>21</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>22</sup> 16 U.S.C. § 824o–1, (b)(4)(c).

<sup>23</sup> 16 U.S.C. § 824o–1, (a)(2).

<sup>24</sup> 16 U.S.C. § 824o–1, (a)(4).

facilities needed to maintain transmission system reliability.”<sup>25</sup> These BPS generation and transmission assets provide synchronized power within the three interconnections that serve the entire United States and parts of Mexico and Canada.<sup>26</sup>

As defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.<sup>27</sup> That limitation creates a potential problem for executing emergency orders. Local distribution systems often provide the “last mile” of connectivity between transmission systems and military bases and other critical customers. As DOE and industry create template emergency orders and execution plans, it will be essential to integrate local distribution providers into that development process.

However, before examining these distribution-level issues, it will first be helpful to clarify the components of the BPS that are explicitly subject to emergency orders under the FPA (and are therefore key partners for DOE in designing them). The FPA states that the secretary of energy may issue emergency orders to the following the BPS “entities:”<sup>28</sup>

**The Electric Reliability Organization.** After blackouts cascaded across major portions of the United States in August 2003, Congress authorized the Federal Energy Regulatory Commission (FERC) to certify an electric reliability organization to develop and enforce, subject to FERC approval, mandatory

electric reliability standards for all users, owners, and operators of the US BPS.<sup>29</sup> FERC certified the North American Electric Reliability Council (NERC) as the first-ever electric reliability organization in July 2006. Renamed the North American Electric Reliability Corporation in 2007, it has served in that role since.<sup>30</sup> NERC’s mission is to ensure the reliability and security of the BPS in North America. As such, NERC is uniquely positioned to help DOE develop emergency orders, especially for attacks that could create cascading blackouts or other multistate disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a leading role for the electricity subsector in establishing situational awareness, incident management and coordination, and communication capabilities.<sup>31</sup> E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be vital for responding to grid security emergencies.

**Regional entities responsible for enforcing reliability standards for the BPS.**<sup>32</sup> NERC has delegated certain authorities to eight regional entities to monitor and enforce compliance with reliability standards.<sup>33</sup> While regional entities play major oversight roles, they do not directly operate the physical grid and would not, on their own, be positioned to execute emergency orders. However, they could help utilities and DOE and preplan for

<sup>25</sup> 16 U.S.C. § 824o, (a)(1).

<sup>26</sup> Interconnections are defined as the “geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control.” North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See NERC, *Glossary*.

<sup>27</sup> The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify “local” distribution. See 16 U.S.C. § 824o, (a).

<sup>28</sup> 16 U.S.C. § 824o–1, (b)(4).

<sup>29</sup> Energy Policy Act of 2005, Public Law 109-58. This does not include Alaska or Hawaii.

<sup>30</sup> NERC, *History*. For more information on NERC, see “About NERC,” NERC.

<sup>31</sup> “Electricity Information Sharing and Analysis Center,” NERC.

<sup>32</sup> DOE, “RIN 1901–AB40,” 1177. See also 16 U.S.C. § 824o, (a)(7).

<sup>33</sup> “Key Players,” NERC. In July 2017, however, one regional entity announced its intention to dissolve. FERC has approved the dissolution, effective July 2018. See FERC, *Order Granting Approvals* (163 FERC ¶ 61,094).

issuing regulatory waivers to BPS grid operators as they comply with emergency orders.

**Owners, users, and operators of critical electric infrastructure or defense critical electric infrastructure within the United States.**<sup>34</sup> Companies that own and operate generation and transmission assets will be among the most likely recipients of emergency orders and should play a critical role in designing them. Reliability coordinators will be similarly important. Reliability coordinators are the entities that constitute “the highest level of authority” for the reliable operation of the bulk electric system (BES).<sup>35</sup> They are also responsible for maintaining a “wide-area view” of the BES and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, reliability coordinators will be critical for designing, receiving, and implementing emergency orders to counter attacks that individual BPS owners and operators may not have the ability to defeat. Seven regional transmission organizations and independent system operators, most of which are registered as reliability coordinators, also help operate and ensure the reliability of the BES in many regions of the United States.<sup>36</sup> Accordingly, regional

transmission organizations and independent system operators will be essential to the design and execution of emergency orders.

### **Local Distribution Providers and Other Grid Resilience Stakeholders**

The 2015 FAST Act amendments to the FPA do not explicitly address the possible roles of local distribution systems in grid security emergencies. However, local distribution infrastructure is critical for overall resilience against cyber and physical attacks. Even if emergency orders help defeat attacks on BPS assets, adversaries may still be able to achieve catastrophic effects by striking multiple local distribution systems and thereby interrupting the flow of power from transmission systems to military bases, hospitals, and other end users. Local distribution systems may also need to help implement emergency orders issued to BPS entities. For example, if the secretary orders transmission systems to protect reliability by shedding load, yet at the same time sustain the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding. Holistic preparedness for grid security emergencies therefore requires engagement with local distribution systems.

These systems will also have strong incentives to participate in the emergency order planning process. Just as BPS entities rely on local distribution utilities, these utilities rely on generation, transmission, and higher-voltage distribution entities to serve end users. Local systems will also share the commitment of BPS entities to protect and rapidly restore service to defense installations and other critical customers. By integrating local distribution utilities

<sup>34</sup> The analysis that follows later in this section examines the definition of “users” of critical electric infrastructure and defense critical electric infrastructure.

<sup>35</sup> While the BPS broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the BES is a subset of the BPS that includes, with some exclusions, all transmission and real and reactive power sources at one hundred kilovolts or higher. As with the BPS definition, the BES definition excludes local distribution providers. For these definitions, as well as the definition of reliability coordinators, see NERC, *Glossary*. Consistent with the FPA and the authorities it provides for handling grid security emergencies, this report focuses on the application of emergency orders to BPS entities specifically.

<sup>36</sup> There are ten regional transmission organizations and independent system operators under NERC’s purview, though three operate exclusively in Canada. Regional transmission organizations and independent system operators are independent membership-based nonprofit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are

operated by individual utilities or utility holding companies. See “About 60% of U.S. Electric Power Supply Managed by RTOs,” US Energy Information Administration. Six of the seven regional transmission organizations/independent system operators operating in the US are also current reliability coordinators. See “Reliability Coordinators,” NERC.

into emergency order planning, these utilities will be able to participate in shaping template orders and implementation plans to help achieve their reliability goals when adversaries strike. Moreover, to the extent that local distribution companies may be subject to emergency orders, they may also benefit from the FPA's liability protections and cost-recovery provisions for actions taken to execute those orders.

DOE and other stakeholders may determine that the FPA already gives the secretary adequate authority to issue emergency orders to local distribution companies. The act states that emergency orders may apply to "any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure" within the United States.<sup>37</sup> The act, however, does not further define owners, users, and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the act.

Regardless of whether the secretary can issue orders to local distribution utilities, BPS entities should include them in building the contingency plans to implement emergency orders. This preplanning will be essential to strengthen comprehensive, end-to-end protection of grid reliability against attacks.

Many companies that own transmission assets also own distribution infrastructure. These utilities will find it relatively easy to include distribution assets in their emergency planning. Integrated response plans will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for "vertically integrated" utilities that own and operate assets for all three functions. However, many municipally owned electric utilities and rural electric cooperatives (including those that serve critical and defense critical electric infrastructure) are not part of vertically integrated companies. In US regions where generation, transmission,

and distribution systems exist as separate entities, additional engagement initiatives will be essential to implement emergency orders and sustain power to essential facilities.

Including state regulators and other state officials in these integrative efforts could offer additional benefits. State public utility commissions have primary regulatory jurisdiction over distribution systems.<sup>38</sup> The National Association of Regulatory Utility Commissioners, which represents state regulators nationwide, has focused growing attention on the need for prudent utility investments in cyber and physical resilience.<sup>39</sup> Commissioners in New Jersey and other states are also leading regulatory initiatives to bolster cyber resilience in their respective jurisdictions.<sup>40</sup> Emergency managers and National Guard leaders in a growing number of states are also building new mechanisms to coordinate with utilities in responding to cyber attacks. Adding such additional partners to help design emergency orders and plan for their implementation would complicate an already far-reaching engagement process. Nevertheless, incorporating perspectives from state commissioners and other officials would help advance comprehensive state-level preparedness for grid security emergencies.

### Additional Partners for Engagement

DOE and power companies will need to collaborate with a wider array of partners to develop and execute some potentially useful emergency orders, especially to support grid restoration. The final rule

<sup>37</sup> 16 U.S.C. § 824o, (b)(4)(a).

<sup>38</sup> The US Constitution, in most cases, allows federal regulation of private economic activity only for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See Lazar, *Electricity Regulation in the US*, 15.

<sup>39</sup> See NARUC, *Cybersecurity*; and NARUC, *Resolution on Physical Security*.

<sup>40</sup> State of New Jersey Board of Public Utilities, *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196).



on *Grid Security Emergency Orders: Procedures for Issuance* (hereinafter referred to as the grid security emergency rule) notes: “Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits” to expedite the restoration of power.<sup>41</sup> This includes traditional partners such as the Department of Homeland Security (DHS) and the Department of Defense (DOD). Still broader collaboration with government and private sector partners may be valuable for implementing emergency orders to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy large power transformers at substations across the United States, and these attacks cut off power to critical military bases, the secretary might order industry to prioritize the replacement of large power transformers at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program to provide for such replacements.<sup>42</sup> New industry-led organizations such as Grid Assurance,<sup>43</sup> as well as programs such as the Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) initiative, are further expanding the industry’s capacity to replace transformers and other equipment.<sup>44</sup> These efforts will be essential for preparing for grid security emergencies, especially as industry stocks and securely stores the full range of replacement transformer types and sizes that large-scale physical attacks may require.

However, power companies do not move large power transformers by themselves. They rely on railroad companies, barges, and heavy-haul trucking companies to help do so and have established a

Transformer Transportation Working Group under the ESCC to plan and coordinate transformer movement.<sup>45</sup> Exercises in the Spare Transformer Equipment Program now involve representation from transportation stakeholders. Yet, the FPA does not give the secretary authority to issue orders to transportation companies. In anticipation of orders for replacing transformers, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Preplanning with the US Department of Transportation (DOT), the Federal Emergency Management Agency (FEMA), and state governments to get contracts, permits, and regulatory waivers to expedite transformer movement will also be useful. In addition, advance coordination with emergency managers at all levels of government would help them mitigate the effects of rotating blackouts or other extraordinary measures on public health and safety.

DOE and the electricity subsector should consider expanding the geographic scope of these discussions as well. In defining the defense critical electric infrastructure that emergency orders can protect, Congress excluded grid assets in Alaska and Hawaii.<sup>46</sup> But both states are home to vital military installations, as are a number of US territories. The secretary also lacks the authority to issue emergency orders to Canadian utilities. Yet, US and Canadian electric systems are deeply integrated, and coordinated efforts to prevent instabilities in grid security emergencies could benefit both nations. Collaborations with NATO allies and other security partners in the face of major adversarial cyber campaigns could be valuable as well. The concluding section of this report examines the potential benefits of expanding grid

<sup>41</sup> DOE, “RIN 1901–AB40,” 1177.

<sup>42</sup> See DOE, *Strategic Transformer Reserve*; and “Spare Transformers,” EEL.

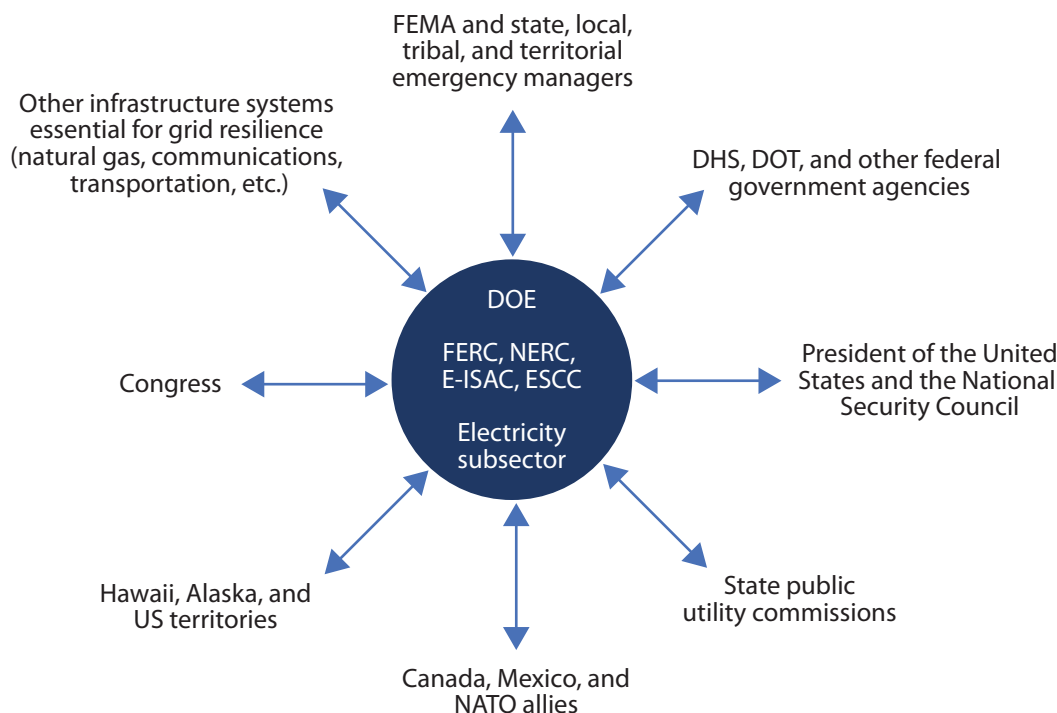
<sup>43</sup> “Transmission Equipment Ready,” Grid Assurance.

<sup>44</sup> FERC, *Order Authorizing Acquisition and Disposition* (163 FERC ¶ 61,005), 10.

<sup>45</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>46</sup> 16 U.S.C. § 824o–1, (a)(4). The FPA’s section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).





**Figure 1. Stakeholders for Building Grid Security Emergency Resilience**

security emergency coordination within the United States and beyond.

Figure 1 illustrates the array of partners that might help build preparedness for such emergencies. DOE, BPS entities, and the broader electricity subsector comprise the core of the team needed to design, issue, and implement emergency orders. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>47</sup> This definition comprises the key subsector components represented in the ESCC, to include owners and operators of electric generation, transmission, and distribution assets “from all ownership categories.”<sup>48</sup> As such, the ESCC is ideally suited to coordinate with

DOE in the order development process, together with NERC, the E-ISAC, and other BPS entities and trade associations.

Surrounding these core participants are additional partners that might offer valuable insights for developing orders and coordinating emergency response operations. Some of these partners (including Congress) can also help oversee the implementation of the FPA’s emergency provisions and assess requirements for further statutory changes.

Of course, the full set of potential contributors to emergency preparedness is broader still. For example, vendors who can help utilities replace damaged relays and other equipment could play vital roles. So could law enforcement agencies, cybersecurity contractors, state National Guard organizations, and other sources of expertise and support for power companies. National laboratories and other research and development organizations will also need to sustain their support for improved grid resilience. Over time, comprehensive engagement with all such partners could pay major dividends.

<sup>47</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>48</sup> In addition to infrastructure owners and operators, ESCC membership includes regional transmission organizations and independent system operators, NERC, the National Infrastructure Advisory Council, and the Canadian Electricity Association. ESCC, *Electricity Sub-Sector Coordinating Council Charter*, 3.

## Goals and Specific Design Requirements for Developing Emergency Orders

The starting point in developing template emergency orders is to identify the objectives, scope, and design requirements that these orders will need to encompass. Key issues analyzed in the sections of the report that follow:

- **Threats, triggers, and thresholds for issuing emergency orders.** Only a limited number of natural and man-made hazards can trigger a grid security emergency.<sup>49</sup> Countering each of those hazards will require threat-specific emergency orders. Hence, the first step for developing such orders will be to examine the threats and attack scenarios on which the design process should focus and clarify the criteria that the president might use to determine that a grid security emergency exists—including when there is an “imminent danger” of an attack.
- **Designing emergency orders for sequential phases of grid security emergencies.** Different types of emergency orders will be needed to protect grid reliability (1) when attacks are imminent, and (2) when attacks are under way. Promising opportunities also exist to develop orders for a third phase of grid security emergency operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.
- **Incorporating national security policies and priorities into emergency order design.** Adversaries may strike the grid to disrupt the flow of power to defense installations and other facilities essential to national security. Many utilities are already collaborating with defense partners to build redundant power feeds for these facilities and make other targeted

investments in resilience. A growing number of grid owners and operators also plan to prioritize the restoration of power to military bases if blackouts occur. Emergency orders provide a unique opportunity for DOE and its partners to build on such initiatives, and provide more systematic, comprehensive, and effective support to national security.

An initial step to do so is to ensure that emergency orders reflect and help achieve broader federal government strategies to defend critical infrastructure. Most important, the US *National Security Strategy* specifies how the United States will deter attacks on critical systems and—if deterrence fails—how it will defeat the attackers.<sup>50</sup> DOE and its industry partners should design emergency orders to help implement the strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this design process with two further steps. First, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. The FPA provisions and existing industry plans to prioritize the restoration of power will provide a useful starting point. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement emergency orders and help defend the nation.

Emergency orders and implementation plans also offer a basis to clarify how US agencies and private companies will coordinate their operations during cyberwarfare, and build consensus on the private sector’s emerging role in national security. No power company has ever tried to maximize shareholder value by promising to bolster cyber deterrence or help defeat attacks by nations such as Russia or China. Yet, because

<sup>49</sup> In addition to being triggered by cyber attacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, (a)(7).

<sup>50</sup> White House, *National Security Strategy*, 13.

of the grid's importance to the economy, public health and safety, and national defense, the United States needs a doctrinal framework to coordinate industry and government actions during attacks on the US electric system.<sup>51</sup> Scott Aaronson, Edison Electric Institute's vice president for security and preparedness, notes that "there is not a lot of doctrine around cyber attacks on civilian infrastructure."<sup>52</sup> Building such doctrine and operationalizing public-private partnerships will be crucial for grid security emergency preparedness.

- **Communications.** The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The grid security emergency rule describes the consultative process that (if practicable) will occur before the secretary issues emergency orders.<sup>53</sup> However, the grid security emergency rule does not address the risk that adversaries will attack the industry-government communications systems necessary to issue orders, monitor their implementation, and defeat adversaries' attacks.

Building secure, survivable communications will be essential to effectively issuing and implementing emergency orders. However, the FPA provides no requirements or funding to do so. The electricity subsector is currently working with government agencies and telecommunications companies to advance secure communications initiatives. These partners should treat preparedness for grid security emergencies as a special area of focus, including measures to

ensure that grid owners and operators can verify the authenticity of emergency orders.

Government and utility leaders will also need to coordinate what they tell the American people when the secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including those for prioritized load shedding, could cut off electricity to many thousands of customers. Emergency orders that will have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Attackers will strike the grid to achieve political benefits, including, potentially, the incitement of public panic and a loss of confidence in US leaders. To promote unity of messaging against such efforts, it will be essential to build on existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders.

- **Waivers and cost recovery.** Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the act itself, FERC-approved reliability standards, or environmental regulations.<sup>54</sup> However, emergency orders will be easier to implement if they include preplanned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

<sup>51</sup> For DOD's definition of doctrine and an analysis of its benefits for joint warfighting, see Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United State*.

<sup>52</sup> Lynch, "How the Russian Government Allegedly Attacks."

<sup>53</sup> DOE, "RIN 1901-AB40," 1181.

<sup>54</sup> These waivers apply unless companies carry out orders and related actions in a "grossly negligent manner." See 16 U.S.C. § 824o-1, (f)(4).

The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.<sup>55</sup> Industry–government dialogue will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader preplanning needed for the financial turbulence that grid security emergencies could create. This study also examines possible emergency orders that would require investments in grid infrastructure to implement. The FPA does not authorize government spending on such pre-emergency projects. If DOE and its partners decide that investment-dependent orders have sufficient value for grid resilience, these partners (and Congress) should explore government funding options that reflect the national security benefits of such orders, rather than increase the electricity bills paid by private citizens.

- **Opportunities for broader resilience against grid security emergencies.** Power companies and DOE may find it helpful to develop a comprehensive plan to sequence and integrate all of the initiatives outlined above. Such a plan might also account for three additional opportunities for progress: (1) employing additional government authorities to coordinate emergency operations between electric utilities and companies in other infrastructure sectors, including the natural gas providers on which power generation increasingly depends; (2) deepening US partnerships with Canada to help protect the interconnected North American power grid, and exploring opportunities for collaboration with Mexico and other nations; and (3) examining longer-term opportunities to leverage improvements in grid resilience to strengthen cyber deterrence, and assessing the risks and potential benefits of coordinating cyber defense operations at home and abroad.

## Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies

The FPA leaves the president substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should build consensus on the types of threats that ought to drive and sequence the development process. These partners should also examine possible decision criteria and consultative mechanisms to support declarations of grid security emergencies.

### Threats That Can Trigger Grid Security Emergencies: Implications for Emergency Order Design

A broad array of natural and man-made hazards, including earthquakes and severe weather events such as hurricanes and ice storms, can cause multistate blackouts. However, in amending the FPA, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the “occurrence or imminent danger” of:

(A)

(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;<sup>56</sup> and

(ii) disruption of the operation of such devices or networks, with significant adverse

<sup>55</sup> 16 U.S.C. § 824o–1, (b)(6).

<sup>56</sup> The second section of this report defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of grid security emergency thresholds.



effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event;

or

(B)

(i) a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and

(ii) significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.<sup>57</sup>

Protecting critical and defense critical electric infrastructure against each of these threats will require different types of emergency orders—though some potential orders may be useful against multiple hazards. The threats will also pose disparate challenges for determining whether a grid security emergency is imminent or under way. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the president faces uncertainties about the likelihood and potential consequences of a grid security emergency.

### Geomagnetic Storms as a Possible Initial Focus

Emergency orders for geomagnetic disturbances will entail fewer design challenges than those for cyber attacks and other man-made hazards, and therefore provide opportunities for rapid progress. Geomagnetic disturbance events occur when coronal mass ejections on the sun create geomagnetically induced currents on the earth's surface. These currents can damage unprotected transformers and other grid infrastructure. Compared with the other threats that can trigger grid security emergencies, determining that there is imminent danger of a geomagnetic disturbance event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the president decide whether

to declare a grid security emergency and will provide significant warning before geomagnetically induced currents threaten to damage grid infrastructure.

Industry and government partners can develop emergency orders to take advantage of this warning time. For example, the secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of geomagnetically induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.<sup>58</sup>

A strong foundation already exists for drafting such orders. Studies of the effects of geomagnetic disturbances on the power grid have contributed to a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.<sup>59</sup> Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the federal government to ensure that it has the capability to predict and detect space weather events and the ability to communicate these assessments to public and private sector stakeholders. The order also requires the development of protection and mitigation plans for critical infrastructure and plans for response and recovery if geomagnetic disturbances occur. In addition, the order requires sector-specific agencies to “assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event.”<sup>60</sup>

NERC reliability standards provide an additional cornerstone for developing emergency orders for geomagnetic disturbances. TPL-007-1—*Transmission System Planned Performance for Geomagnetic*

<sup>58</sup> Phillips, “Solar Shield.” See also MISO, *Geomagnetic Disturbance Operations Plan*, 5.

<sup>59</sup> See “NOAA Space Weather Scales,” NOAA; and Kappenman, *Geomagnetic Storms*.

<sup>60</sup> Obama, *Executive Order—Coordinating Efforts*.

<sup>57</sup> 16 U.S.C. § 824o–1, (a)(7).



*Disturbance Events* establishes long-lead geomagnetic disturbance planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat for geomagnetic disturbance events.<sup>61</sup> EOP-010-1—*Geomagnetic Disturbance Operations* also requires reliability coordinators to develop geomagnetic disturbance mitigation plans and operating procedures, including specific actions that transmission operators must take based on predetermined geomagnetic disturbance-related conditions.<sup>62</sup>

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyber attacks and other man-made triggers for grid security emergencies. The sun will not intentionally hide preparations for a geomagnetic disturbance event or “prepare the battlefield” by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data that utility personnel need to maintain situational awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of critical and defense critical electric infrastructure.

The relative ease of drafting orders for geomagnetic disturbances makes such efforts a prime starting point for industry–government collaboration. The North American Transmission Forum, in coordination with the ESCC, is already examining opportunities to develop template emergency orders for geomagnetic disturbance events. But the greater degree of difficulty associated with protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of emergency orders to counter such threats. Instead,

DOE and its industry partners should consider pursuing a multitrack development process: at the same time that they seek rapid progress on emergency orders for geomagnetic disturbances, they should *immediately* accelerate the long-lead work that will be required to counter each of the man-made threats that can trigger grid security emergencies.

### Cyber and Physical Attacks

This report focuses on supporting the development of emergency orders to protect and restore grid reliability against cyber and physical attacks. In doing so, the report follows the lead of the premier electric industry exercise of grid resilience, GridEx. As in previous versions of this exercise series, GridEx IV (conducted in November 2017) employed a scenario based on large-scale, combined cyber and physical attacks against the US electric system by a highly capable adversary.<sup>63</sup> Such combined attacks could pose severe threats to nationwide grid reliability, over and above those created by cyber or physical strikes alone. Grid security emergency orders that can help power companies protect and restore reliability against combined attacks will be especially valuable for national security. Orders and implementation plans that can help counter such severe threats will also be useful in lesser contingencies, including cyber-only strikes.

Current US policy priorities focus on the need to strengthen cyber resilience for the power grid and other critical infrastructure. The US *National Security Strategy* warns that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>64</sup> DOE and its partner utilities should prioritize the development of emergency

<sup>61</sup> NERC, *TPL-007-1*.

<sup>62</sup> The standard, however, does not explicitly lay out what those predetermined conditions should be. See NERC, *EOP-010-1*. For an example of geomagnetic disturbance plans, see PJM, *PJM Manual* 13, 69–71.

<sup>63</sup> GridEx includes participation by over one hundred power companies and other components of the electricity subsector. See NERC, *Grid Security Exercise GridEx IV*, vii.

<sup>64</sup> White House, *National Security Strategy*, 12, 27.

orders to counter such attacks, and supplement the mandatory and increasingly stringent cyber critical infrastructure protection standards, as well as voluntary measures that go above and beyond those NERC requirements.<sup>65</sup>

However, orders can also help build resilience against physical attacks on the grid. Since the coordinated attack on the Metcalf substation near San Jose, California, in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high-powered rifles or other weapons. This includes NERC's *CIP-014-2—Physical Security* standard, which outlines the requirements for protecting grid infrastructure from physical attacks.<sup>66</sup> Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide-area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

An adversary would face greater risks when launching physical attacks than cyber attacks. Blowing up transformers and killing workers who are transporting replacement equipment might rapidly escalate conflict with the United States into larger-scale kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries would hide on utility networks, arming and prepositioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages that last far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk-reward calculus in our favor. If orders can help power companies protect their systems from impending physical attacks, especially in partnership with state and local law enforcement agencies, state National Guard personnel, and other sources of assistance, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Adversaries may also simultaneously employ both cyber and physical attacks. Such combined attacks can synergistically disrupt the grid in ways that cyber or physical attacks on their own cannot. For example, as in the response to cyber attacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.<sup>67</sup> However, physical attacks that destroy critical substation components or target utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

The GridEx IV scenario highlighted the unique challenges posed by combined attacks and opportunities to address them. That scenario also assumed that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging that are far more difficult to counter than in any past US power outage.

This report adopts a similarly severe threat for analyzing possible emergency orders. In particular, the report examines how orders can protect or restore grid reliability against the combined use of cyber weapons, physical attacks, and information

---

<sup>65</sup> NERC has mandatory standards for critical infrastructure protection against cyber threats. See "United States Mandatory Standards," NERC.

<sup>66</sup> DOE, *Quadrennial Energy Review*, 4–34; and NERC, *CIP-014-2*.

---

<sup>67</sup> E-ISAC and SANS-ICS, *Analysis of Cyber Attack*, v.

warfare against critical and defense critical electric infrastructure. Of course, separate types of emergency orders will be required for physical and cyber threats. Orders to deploy specific countermeasures against unmanned aerial vehicle attacks on substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead, utilities can also benefit from examining how emergency orders could help them defeat combined attacks, and how they can integrate both cyber and physical defense operations.

The study does not examine options for developing emergency orders against electromagnetic pulse (EMP) attacks. EMP threats pose a significant potential risk to the grid, and a growing (though still relatively small) number of utilities are hardening their critical systems against EMP effects.<sup>68</sup> DOE's EMP strategy provides a valuable framework and approach for managing the risks that EMP threats pose to the grid and other energy systems.<sup>69</sup> DHS's EMP strategy does the same for a broad range of infrastructure sectors.<sup>70</sup> Industry partners such as the Electric Power Research Institute are also making notable contributions to the shared understanding of EMP effects on the grid.<sup>71</sup> However, significant

research is still required to understand the combined effects of EMP wave components on grid hardware and system-wide operations and for cost-effective mitigation options and preparedness planning.<sup>72</sup> As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

## Thresholds for Declaring Grid Security Emergencies<sup>73</sup>

The FPA authorizes the president to declare a grid security emergency when there is "imminent danger" of an attack or when attacks are already occurring. However, the FPA does not further define imminent, nor provide any criteria to help determine whether the anticipated likelihood of an attack is sufficient to warrant an emergency declaration. As will be discussed below, the FPA provides guidance on the potential severity of imminent or ongoing attacks that would constitute a grid security emergency. However, those guidelines are broad and could be subject to starkly different interpretations in future crises.

Some degree of ambiguity is useful. Preserving wide presidential latitude for declaring grid security emergencies will be essential to deal with unforeseen challenges and to avoid locking US crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicize explicit red lines that would trigger a declaration. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay US defensive measures, including the issuance of emergency orders to safeguard the grid. Adversaries might even seek to spoof the president into declaring a grid security emergency when they had no intention of launching an attack—especially if adversaries believed doing so might prompt the issuance of disruptive emergency orders, crash utility stock

<sup>68</sup> In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to geomagnetic disturbances. The early-time component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See EPRI, *Electromagnetic Pulse and Intentional EMI Threats*, 3-3–3-4.

<sup>69</sup> DOE set strategic goals for addressing EMP threats and created an action plan to meet those goals. DOE, *Electromagnetic Pulse Resilience Action Plan*. The fiscal year 2017 National Defense Authorization Act directed DHS to create a similar strategy, which is currently in draft form. See National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328. The EPRI continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse*.

<sup>70</sup> DHS, *Strategy for Protecting and Preparing*.

<sup>71</sup> EPRI, *Electromagnetic Pulse and Intentional EMI Threats*.

<sup>72</sup> INL, *Strategies, Protections, and Mitigations*.

<sup>73</sup> The analysis in this section builds on the findings of Stockton, "Thresholds."

prices, or incite public panic in ways that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events that emergency orders should be designed to help counter.<sup>74</sup> Federal officials could also find it useful to have decision criteria to help frame their own internal deliberations and recommendations to the president. In an intense crisis, ambiguities in the FPA could fuel disagreements among the president's advisors as to whether the threat of attack was sufficiently severe to declare a grid security emergency. Developing a decision framework to support the declaration process could facilitate consensus-building and provide a structured way to integrate data on attack indicators. However, in adopting such a framework, it would also be prudent to avoid revealing any specific declaration triggers or thresholds for adversaries to exploit in their attack planning.

The section that follows examines two factors that a decision framework might encompass: the likelihood of an attack occurring and its potential consequences. This section also examines how improved information sharing between government agencies and power companies can support these assessments and recommends industry–government consultations in the declaration process that go beyond the existing provisions of the FPA.

### **Determining When Attacks Are Imminent: Criteria for Declaring Grid Security Emergencies**

In key respects, the BPS is under cyber attack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant advanced persistent threats on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS networks, secrete malware

designed to disrupt grid operations, and conduct other malicious activities to prepare for possible attacks on critical system components.<sup>75</sup> PJM Interconnection's former CEO Terry Boston recently stated that the company experiences three thousand to four thousand hacking attempts *every month*.<sup>76</sup> Penetration efforts on a similarly massive scale are likely occurring against BPS entities across the United States. While many of these efforts target information technology systems not directly involved in operating the grid, malware implants on operational technology systems are increasingly frequent and sophisticated.<sup>77</sup> And, as in the case of BlackEnergy and other campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.<sup>78</sup> The net result, according to US director of national intelligence Dan Coats: "Today, the digital infrastructure that serves this country is literally under attack."<sup>79</sup>

Of course, there is a huge gulf between implanting destructive malware on the grid and using that malware to create blackouts. The Trump administration has promised to impose "swift and costly consequences" on foreign governments and other actors who undertake "significant malicious cyber activities" against US critical infrastructure.<sup>80</sup> Attacks that create massive power outages and jeopardize US national security would be especially likely to provoke such a response. However, the president does not need to wait for blackouts to occur before declaring

<sup>75</sup> "Alert (TA18-074A)"; "Alert (TA17-293A)"; Defense Science Board, *Task Force on Cyber Deterrence*, 4; and ICF International, *Electric Grid Security and Resilience*, 19.

<sup>76</sup> Dougherty, "Biggest U.S. Power Grid Operator Suffers Attacks."

<sup>77</sup> "Alert (TA17-293A)"; and "Alert (TA18-074A)."

<sup>78</sup> BlackEnergy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of BlackEnergy inflicted the 2016 blackout on Ukraine. "Alert (ICS-ALERT-14-281-01E)."

<sup>79</sup> Barnes, "Warning Lights."

<sup>80</sup> White House, *National Security Strategy*, 13.

<sup>74</sup> Paradise et al., "ISO-RTO Council Comments," 2.



a grid security emergency. The “imminent danger” of attack is sufficient to declare an emergency and for the secretary to issue orders to help utilities ramp up their defenses.

Implants of new, potentially devastating malware across the electric grid could help the president make such a determination, particularly if other warning indicators suggest that cyber attacks are becoming increasingly likely. The geopolitical context in which cyber attacks might occur provides one such indicator. It is (barely) conceivable that adversaries will launch a “bolt from the blue” attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region and attack the grid to disrupt the deployment of US forces to the region or to achieve other military and political goals.<sup>81</sup> Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause multistate blackouts, should carry greater weight in a crisis environment.

Policy makers should consider developing a framework to assess whether these cyber preparations help justify the declaration of a grid security emergency. The US Office of the Director of National Intelligence (ODNI) has issued a cyber threat framework that could support such development efforts. The ODNI notes that government agencies, academia, and the private sector are using over a dozen analytic models to categorize cyber threats and identify changes in the activities of cyber adversaries. ODNI’s framework is intended to provide a common basis for characterizing threat activity to support analysis and senior-level decision-making.<sup>82</sup> Figure 2 illustrates the cyber threat framework.

<sup>81</sup> The section on preattack grid security emergency declarations examines these national security-related issues and their implications for designing emergency orders.

<sup>82</sup> “Cyber Threat Framework,” ODNI; and ODNI, *Common Threat Framework*, 5.

The initial stage of adversary activity is to prepare for conducting malicious activity. Adversaries then engage and establish presence on targeted systems, allowing them to “operate at will.” In the final stages, attackers seek to destroy grid hardware, software, and/or data, and prepare to conduct follow-on operations as needed to magnify the extent and duration of their disruptive effects.<sup>83</sup>

If adversaries were to suddenly make new moves into the penultimate phase (operate at will) during an intense political crisis or regional confrontation, evidence that they had done so could help the president determine whether attacks were imminent. Other independent sources of data could provide additional context for assessing adversary moves toward more threatening preattack stages. James Miller, former undersecretary of defense for policy, notes that “the United States devotes massive resources to human and technical intelligence collection of our potential adversaries.”<sup>84</sup> Such indicators could contribute to overall assessments of attack imminence.

Policy makers might also supplement the cyber threat framework with specialized attack models for the industrial control systems and other grid components that are crucial for electric system operations. The Industrial Control System Cyber Kill Chain provides an especially promising opportunity to do so. The kill chain identifies the specific sequenced phases that adversaries execute to conduct attacks that inflict predictable physical effects on grid equipment and operations.<sup>85</sup> Stage 1 begins with planning and reconnaissance against

<sup>83</sup> ODNI, *Common Threat Framework*, 13, 16.

<sup>84</sup> Miller, “Cyber Deterrence.”

<sup>85</sup> The Industrial Control System Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin in 2011 to “help the decision-making process for better detecting and responding to adversary intrusions.” The Industrial Control System Cyber Kill Chain tailors that decision-making tool for industrial control system-specific cyber threats and consequences. See Assante and Lee, *Industrial Control System Cyber Kill Chain*.



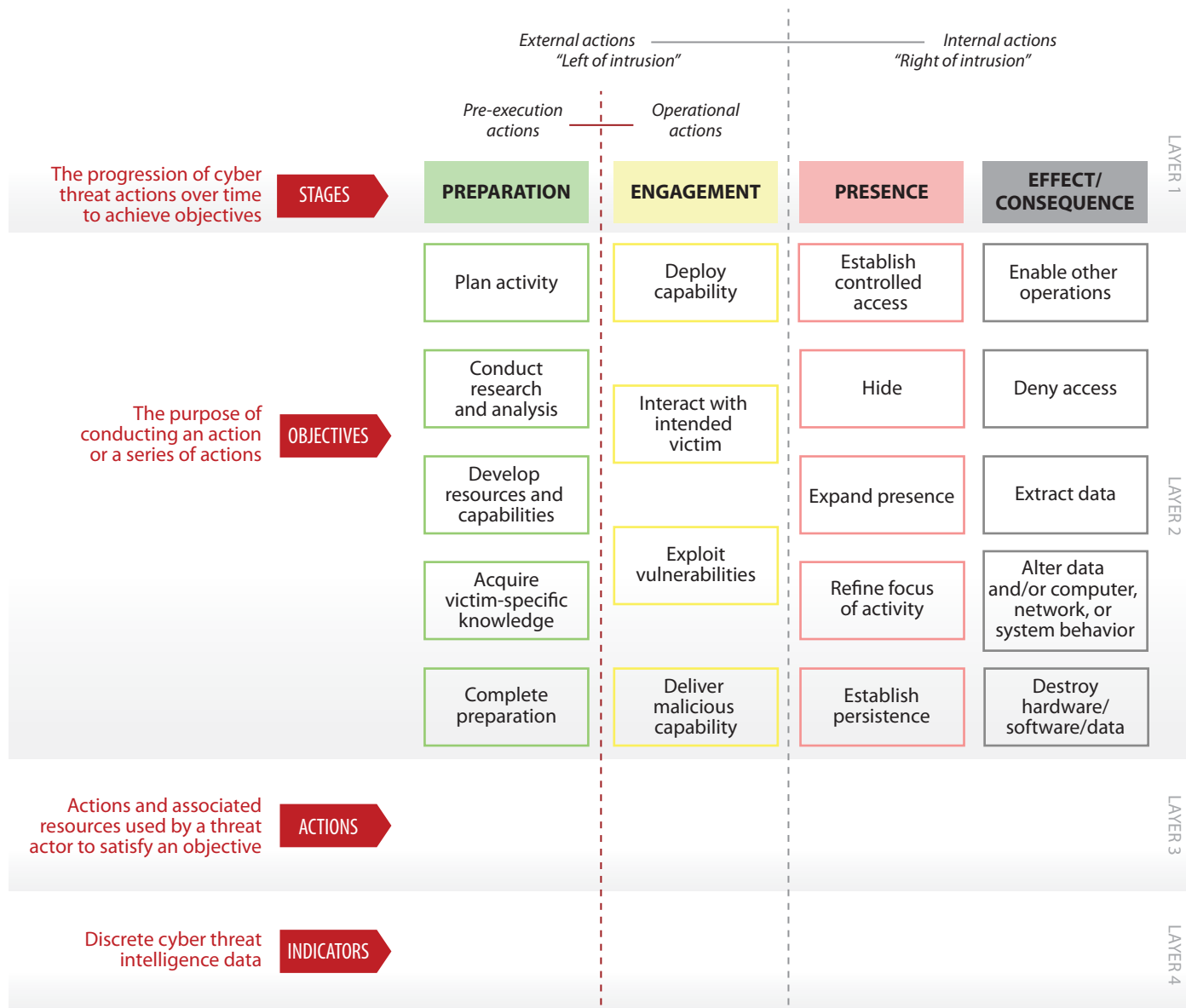


Figure 2. ODNI Cyber Threat Framework

industrial control system networks and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing attack capabilities, and—ultimately—executing the attack. Evidence of an adversary's position along this kill chain could help support decision-making on the imminence of potential attacks, with the final phases posing the most proximate indications that an adversary is poised to strike the grid.

### Potential Attack Consequences

The imminence of an attack provides only one possible criterion for declaring a grid security emergency. A second would be the potential consequences of the attack. Indeed, when Congress defined grid security emergencies in the FPA, legislators established at least implicit, consequence-based thresholds for declaring an emergency. The FPA defines grid security emergencies as occurring when attacks that are imminent or under way "could disrupt the

	General Definition	Observed Action	Intended Consequence
Level 5: Emergency (Black)	<i>Poses on imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons</i>	Effect	Cause physical consequence
Level 4: Severe (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties</i>	Presence	Damage computer and networking hardware
Level 3: High (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>	Engagement	Corrupt or destroy data  Deny availability to a key system or service
Level 2: Medium (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Steal sensitive information
Level 1: Low (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Commit a financial crime
Level 0: Baseline (White)	Unsubstantiated or inconsequential event	Preparation	Nuisance denial of service or defacement

Figure 3. Elements of the Cyber Incident Severity Schema

operation” of devices or networks that are “essential to the reliability of critical electric infrastructure or defense critical electric infrastructure.”<sup>86</sup>

However, the FPA does not clarify the extent of disruption that should trigger the declaration of an emergency. Some grid resilience stakeholders have expressed concern that policy makers might set the threshold too low, and declare grid security emergencies for minor incidents. For example, the ISO/RTO Council proposes that the use of emergency orders in such an emergency “should be reserved for true widespread emergencies.”<sup>87</sup> But

neither Congress nor DOE have yet specified what higher-level thresholds might be appropriate.

One approach to account for the potential consequences of an attack would be to leverage existing federal criteria for categorizing cyber events by the severity of their effects. The definition of “significant cyber incidents” in Presidential Policy Directive 41, *United States Cyber Incident Coordination*, provides a starting point to do so. Under the directive, significant cyber incidents are those that are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or

<sup>86</sup> 16 U.S.C. § 824o–1, (a)(7).

<sup>87</sup> Paradise et al., “ISO-RTO Council Comments,” 2.

public health and safety of the American people.”<sup>88</sup> Policy makers could apply this demonstrable-harm standard to support decisions on whether to declare a grid security emergency. If officials determine that a cyber attack is likely to inflict such harm, their finding would provide a compelling justification for making an emergency declaration.

The December 2016 *National Cyber Incident Response Plan*’s cyber incident severity schema offers a still more detailed basis to assess attack consequences. The schema (Figure 3) serves as “a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments” and agencies.<sup>89</sup> Policy makers could use the schema to help develop consequence-based criteria for declaring grid security emergencies. For example, if assessments suggest that an attack is likely to create a “level 5 emergency,” which poses “an imminent threat to the provision of wide-scale critical infrastructure services, national [government] stability, or to the lives of U.S. persons,” the declaration of a grid security emergency should be near-automatic. Level 4 events would also be very strong candidates for justifying such declarations. However, as with all such criteria, the president should also retain the latitude to make declarations for less severe incidents (for example, the disruption of a cluster of major defense installations).

One advantage of leveraging these government-wide standards is that doing so can help integrate decisions on grid security emergencies into the broader US system for incident response. As officials update the *National Cyber Incident Response Plan* and its supporting severity schema, valuable opportunities will emerge to ensure that grid security emergency declarations and operations are part of a broader, multisector approach to strengthening infrastructure preparedness.

### **Grid-Specific Criteria for Assessing Attack Consequences: Building on Standards for Adequate Levels of Reliability**

If policy makers rely only on general, government-wide decision criteria, they will miss opportunities to take advantage of the electric industry’s standards for assessing the severity of threats to grid reliability. NERC has carefully defined what constitutes adequate reliability for the power grid, as well as the types of large-scale reliability failures that owners and operators need to prevent. If utilities and government agencies have the data and analytic tools necessary to determine whether adversaries’ attacks will create such failures, their assessments could provide valuable input into decisions on declaring grid security emergencies.

The 2003 Northeast blackout spurred NERC’s efforts to define adequate levels of grid reliability and specify the types of system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over wide areas of the United States and Canada, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The 2005 amendments required FERC to certify an electric reliability organization, which will have “the ability to develop and enforce . . . reliability standards that provide for an adequate level of reliability of the bulk-power system.”<sup>90</sup> However, the FPA never defined *adequate level of reliability*; that task was left to the electric reliability organization.

When NERC became the electric reliability organization in 2006, defining the adequate level of reliability was one of its first initiatives. NERC’s board of trustees approved an initial definition for the “characteristics of a system with an adequate level of reliability” in 2008, which was updated in 2013.<sup>91</sup> Three components of NERC’s definition—cascading failures, uncontrolled separation, and instability—are

<sup>88</sup> Obama, *United States Cyber Incident Coordination*.

<sup>89</sup> DHS, *National Cyber Incident Response Plan*, 29–30.

<sup>90</sup> 16 U.S.C. § 824o, (c)(1).

<sup>91</sup> NERC, *Technical Report*, 17.

especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS.<sup>92</sup>

The sections that follow examine these three components, the reliability failures they can entail, and implications for declaring grid security emergencies. Subsequent portions of the report analyze options to develop emergency orders tailored to prevent such failures. However, in grid security emergencies, risks of all three types of failures might emerge in rapid succession and would be inextricably linked.

**Cascading failures.** NERC defines cascading as “the uncontrolled successive loss of system elements triggered by an incident at any location.” Such cascading “results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.”<sup>93</sup> NERC’s definition states that a system is adequately reliable if the system will not experience cascading failures when struck by lightning or affected by other frequent, predictable incidents (i.e., “predefined Disturbances”). But more severe events have caused instabilities that led to cascading in the past and may do so again—especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout illustrates the speed with which failures can cascade. That blackout, which affected approximately fifty million people across the United States and Canada, started with a relatively minor incident. On a hot day in August, multiple 345-kilovolt transmission lines tripped after sagging into overgrown trees. With proper situational awareness, operators might have been able to take actions to handle such a contingency, but failures in

the utility’s control room alarm processor resulted in operators being entirely unaware of the problem. In an unfortunate coincidence, the utility’s reliability coordinator also had computer problems and lacked the visual tools necessary to support grid operators.<sup>94</sup> These failures shifted power flows to a system of 138-kilovolt lines, which were unable to handle the added current flows, and overloaded the last remaining 345-kilovolt path into the area, beginning the major, uncontrollable cascading sequence.<sup>95</sup> This sequence tripped over five hundred generating units and four hundred transmission lines in only eight minutes—with most of these failures occurring *in the last twelve seconds* of the cascade.<sup>96</sup>

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversarial attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying critical generation and transmission nodes; alter protective relay settings so that grid components trip offline (or fail to do so) in ways that intensify the outages; deny grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and take other measures designed to produce cascading failures.<sup>97</sup> Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe—particularly by denying or corrupting situational awareness data.

The imminent danger or occurrence of adversary-induced cascading outages could be a criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt

<sup>92</sup> See section 215 of the FPA, which defines *reliable operation* as “operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” 16 U.S.C. § 824o, (a)(4).

<sup>93</sup> NERC, “Informational Filing,” 1, 7.

<sup>94</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>95</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>96</sup> NERC Steering Group, *Technical Analysis of Blackout*, 109.

<sup>97</sup> Cherepanov and Lipovsky, “Industroyer”; Sistrunk, “ICS Cross-Industry Learning”; “Alert (TA17-163A)”; and Dragos, *CRASHOVERRIDE*, 24.

the operation of grid devices and networks essential to critical and defense critical electric infrastructure—on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

**Uncontrolled separation.** NERC defines uncontrolled separation as “the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss.”<sup>98</sup> Severe events “resulting in the removal of two or more BES elements with high potential to cascade” can produce uncontrolled separation.<sup>99</sup>

Uncontrolled separation almost always occurs in conjunction with cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands that “quickly became unstable after the massive transient swings and system separation” because there was insufficient generation within the islands to meet electricity demand.<sup>100</sup> Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.<sup>101</sup> In the 1982 West Coast blackout, loss of 500-kilovolt lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, dividing the system into four unplanned islands.<sup>102</sup> A similar blackout in the same region in 1996, triggered by multiple major transmission line outages, again separated the Western Interconnection into four electrical islands

“with significant loss of load and generation.”<sup>103</sup> The onset of adversary-induced uncontrolled separation would provide a clear-cut basis for declaring the existence of a grid security emergency, if cascading failures had not already prompted the president to make such a determination.

**Instability.** NERC defines system instability as “the inability of the Transmission system to remain in synchronism . . . characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES.”<sup>104</sup> The BES can experience frequency, voltage, or angular instability—though none should occur during normal operating conditions.<sup>105</sup>

Severe natural hazards and other disturbances can create temporary instabilities. Grid protection systems and operational protocols typically mitigate their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, the transmission system may experience large power swings if BPS generators accelerate or decelerate too much during a disturbance, causing transmission lines to trip and generators to go out of step and trip offline, and resulting in further acceleration and deceleration—or both.<sup>106</sup> Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread cascading failures. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur. Corrupting or disabling protection systems could also make critical grid components vulnerable to physical damage from enemy-induced power surges.

<sup>98</sup> NERC, “Informational Filing,” 6.

<sup>99</sup> NERC, “Informational Filing,” 13.

<sup>100</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 75.

<sup>101</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 104.

<sup>102</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 105.

<sup>103</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 106.

<sup>104</sup> NERC, “Informational Filing,” 6.

<sup>105</sup> NERC, “Informational Filing,” 1–2.

<sup>106</sup> NERC, “Informational Filing,” 6.



Evidence that adversaries were taking preparatory measures to create widespread instabilities could help the president determine that a grid security emergency exists.

However, it may be difficult to predict whether an impending attack will create such failures. The first requirement to do so will be to determine the extent to which adversaries have embedded advanced persistent threats or established other means of attack across the grid—a task that adversaries will complicate by attempting to hide their malware from detection. The next step will be to rapidly characterize these threats, assess the vulnerability of utility systems to them, and predict the consequences for grid reliability if the enemy strikes. Such assessments will also need to account for system-wide effects involving the interaction of multiple adversary-induced disruptions, which may compound and reinforce instabilities in ways that are difficult to predict. PJM Interconnection, LLC, the regional transmission operator for much of the Mid-Atlantic and some neighboring states, recently noted that “additional study is needed to better understand the expected impacts of a large-scale cyber-attack.”<sup>107</sup> Given these challenges, it may be difficult to fully predict the potential impact of cyber attacks on grid reliability until attacks are well under way.

But it could also be risky to wait until attacks are occurring to declare a grid security emergency. In the 2003 Northeast event, for example, cascading blackouts spread across vast areas in seconds. If the president delays declaring a grid security emergency until cascades are under way, emergency orders designed to help prevent their spread may come too late. A better option might be to make an early decision based on imperfect assessments, especially if (as this report recommends) DOE can issue preattack emergency orders that will bolster grid defenses without disrupting normal electric service.

In particular, the president could consider declaring a grid security emergency if (1) an attack appears to be increasingly likely, and (2) assessments indicate that the impending attack may create cascading blackouts or other widespread instabilities. Figure 4 illustrates one option for developing a decision support framework that accounts for the likelihood and potential consequences of an attack. The vertical axis depicts the ODNI cyber threat framework’s four stages of adversary actions, from potential attack preparations to actual strikes against the grid. An adversary’s sudden, large-scale moves up this axis—especially in the context of a severe international crisis—could help the president determine that an attack is impending. The horizontal axis represents the risk that if an attack occurs, the grid will experience cascading failures and other widespread instabilities that would inflict demonstrable harm to national security, the economy, or public health and safety. Attacks that pose little or no risk of cascading blackouts might not warrant the declaration of a grid security emergency.

However, systemic threats to grid reliability are far from the only consequence-based criteria that the president might want to consider. More narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security, such as the National Capital Region, might be sufficient to declare a grid security emergency. Policy makers could develop more refined decision frameworks to account for a broad array of consequence thresholds, as well as further criteria for assessing attack imminence.

## Data Sharing and Consultations with Industry

The electric industry can provide data and analytic support to help the president and other officials decide whether to declare a grid security emergency. Power companies will have direct access to the malware that adversaries implant on their networks, and will be well positioned to assess the potential

<sup>107</sup> PJM, “Comments and Responses,” 35.

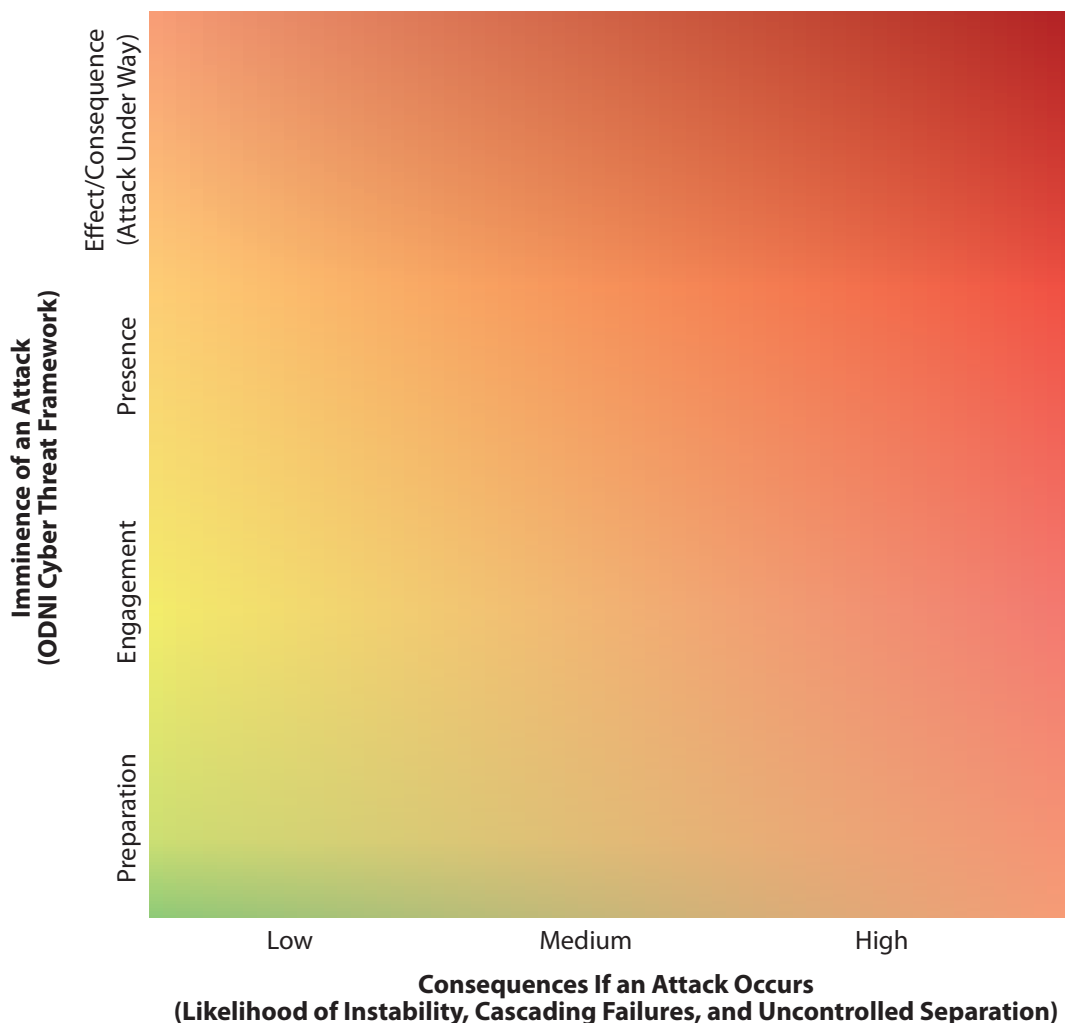


Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies

impact of various attack vectors on their systems and on the grid as a whole.

Government agencies and cyber contractors can help utilities target searches for this malware and provide additional value for the declaration process. If a regional crisis or other geopolitical factors increase the risk of cyber attacks on the grid, agencies should be prepared to ramp up information sharing with BPS entities, especially in terms of specific signatures or other threat indicators to search for in utility networks, logs, and critical equipment.

Industry and government should also explore how ongoing threat detection and analysis initiatives could directly help assess the imminence and

potential consequences of attacks. For example, DOE has projects under way to bolster situational awareness for operational technology networks that could be applied to support such assessments. The department is developing capabilities to monitor traffic on operational technology networks via the Cybersecurity for the Operational Technology Environment project.<sup>108</sup> Other department-funded projects could prove useful for the emergency declaration process as well.<sup>109</sup>

<sup>108</sup> DOE, *Multiyear Plan*, 23.

<sup>109</sup> See, for example, the Containerized Application Security for Industrial Control Systems, Survivable Industrial Control Systems, and Research Exploring Malware in Energy Delivery Systems projects. “Sandia’s Grid Modernization Program

Utilities and DOE might also refine ongoing information sharing initiatives to directly support the emergency declaration process. For example, DOE's Cybersecurity Risk Information Sharing Program is a public-private partnership to build bidirectional situational awareness and facilitate classified and unclassified information sharing.<sup>110</sup> DOE's 2018 cybersecurity plan launched additional activities to advance industry participation in the program, as well as its analytic tools and capabilities.<sup>111</sup> The program is managed by NERC and the E-ISAC, which play an integral role in sharing information and establishing situational awareness within the electricity subsector.<sup>112</sup> In addition, FERC recently issued a proposed directive for NERC to expand reporting requirements for cyber incidents, including for those that "might facilitate subsequent efforts to harm the reliable operation of the bulk electric system."<sup>113</sup> All of these efforts could be integrated to support assessments of the likelihood and potential consequences of attacks.

DHS's May 2018 cybersecurity strategy provides a broader approach to expand information sharing. Most important, the strategy could enable data from other infrastructure sectors to support the declaration process, especially from communications systems and other sectors that support power restoration operations. The strategy also calls for the expansion of automated mechanisms to receive, analyze, and share cyber threat indicators, defensive measures, and other cybersecurity information with critical infrastructure and other key stakeholders.<sup>114</sup>

Such automated sharing mechanisms will be vital to accelerate the identification and assessment of malware that could pose imminent threats to grid reliability. DHS's Automated Indicator Sharing capability "enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed."<sup>115</sup> This bidirectional information sharing will limit an adversary's ability to compromise multiple systems with the same malicious code. The Defense Advanced Research Projects Agency is also working on new technologies to protect the grid. In particular, the agency's Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is working with companies to develop prototype capabilities for improving attack detection, response, and forensics support.<sup>116</sup> Moreover, as automated malware detection and analytic techniques improve, utilities may be able to speed their evaluation of potential intrusions and slash the number of false positives that current detection systems generate.<sup>117</sup> All of these initiatives should be leveraged to help the president determine whether to declare a grid security emergency.

Policy makers should also consider preplanning to consult with grid owners and operators in the declaration process. The FPA leaves the president with sole authority to declare a grid security emergency. If a potential emergency surfaced, the president would almost certainly draw on the expertise and recommendations of the secretary of energy, as well as other members of the National Security Council and supporting agencies. But power companies and their industry organizations will also have perspectives on operational and technical issues that could prove valuable for assessing potential attacks.

---

Newsletter," Sandia National Laboratories; and "REMEDIYS," Cyber Resilient Energy Delivery Consortium.

<sup>110</sup> "Energy Sector Cybersecurity Preparedness," DOE.

<sup>111</sup> DOE, *Multiyear Plan*, 23.

<sup>112</sup> "Electricity Information Sharing and Analysis Center," NERC.

<sup>113</sup> FERC, *Cyber Security Incident Reporting Reliability Standards* (161 FERC ¶ 61,291), 2.

<sup>114</sup> DHS, *Cybersecurity Strategy*, 13.

---

<sup>115</sup> "Automated Indicator Sharing (AIS)," US-CERT.

<sup>116</sup> Douris, "DARPA Research."

<sup>117</sup> Ucci, Aniello, and Baldoni, "Survey on Machine Learning," 1:5; McElwee et al., "Deep Learning"; and McElwee, "Probabilistic Cluster."

Neither the FPA nor the grid security emergency rule explicitly provide for consultations with industry on whether to declare a grid security emergency. The FPA calls for consultations “to the extent practicable” before the secretary issues emergency orders.<sup>118</sup> But there are no equivalent provisions to include industry input in the emergency declaration process.

Industry and government partners should explore options to provide for such consultations, preferably by leveraging existing mechanisms under the ESCC and E-ISAC. As with consultations on issuing orders, urgent circumstances could shorten or preclude opportunities for government dialogue with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of “bolt from the blue” attacks. Nevertheless, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be invaluable for determining whether (and when) to declare a grid security emergency.

## Grid Security Emergency Phases and Order Design Options

DOE and its industry partners should consider designing emergency orders for three potential phases of grid security emergencies. First, if the president determines that there is an imminent danger of an attack, the secretary should be ready to issue preattack orders that help utilities protect grid reliability. Second, once attacks are under way, the secretary could issue orders to reduce the risk of cascading failures or other widespread disruptions of electric service. Third, as utilities begin to restore grid reliability, orders could help utilities replace damaged equipment and counter adversary efforts to disrupt restoration operations.

Orders for each phase of a grid security emergency will differ not only in terms of when the secretary would issue them but also in the degree to which they

will disrupt normal electric service. Some orders, such as staffing up emergency operations centers before an attack occurs, would leave customers unaffected. In contrast, orders for prioritized load shedding could temporarily halt service to many customers—but could also greatly reduce the risk that instabilities will lead to cascading blackouts.

Figure 5 provides examples of orders that vary in the degree of disruption they would inflict on normal service, and also in the way they would meet the phase-specific challenges of grid security emergencies. The analysis that follows examines each of them (and other possible orders) in greater detail.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, emergency orders for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are under way. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies “stop the bleeding” from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are under way.<sup>119</sup> Adversaries may also launch follow-on attacks once utilities begin focusing on restoration. Emergency orders to help utilities repel such attacks could become essential components of the restoration process.

<sup>118</sup> 16 U.S.C. § 824o–1, (b)(3).

<sup>119</sup> In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is fully restored to pre-event conditions) as the “new normal”—characterized by “degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months.” See Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

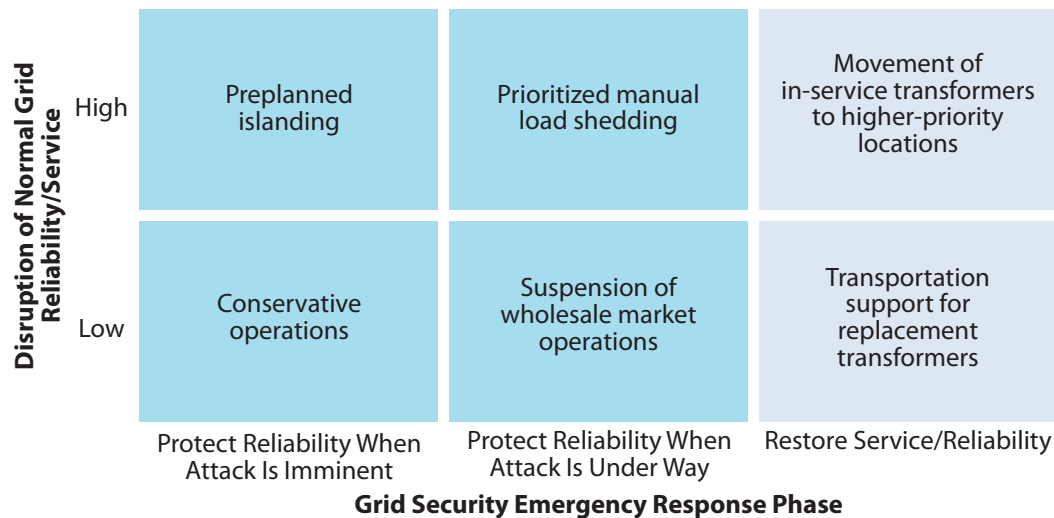


Figure 5. Emergency Order Matrix: Examples of Order Designs

DOE and its partners will need flexibility to deal with the overlapping phases of grid security emergencies. Nevertheless, being able to categorize potential orders in terms of when they would likely be issued and which phases of emergency operations they could support can help establish a systematic process for developing orders.

Creating emergency orders for all three phases can also help utilities and DOE integrate the orders into seamless, multiphase operational plans for grid security emergencies. As intense regional crises or other events elevate the risk of attacks on the grid, it will be prudent to preplan for the issuance of emergency orders for multiple grid security emergency phases. Orders for preattack measures such as conservative operations would be issued first if attacks are deemed imminent. At the same time, however, DOE and the utilities subject to emergency orders should be using any available warning time to prepare for the issuance and implementation of orders for the midattack and restoration phases.

## Preattack Options

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal

with these ambiguities is to delay the declaration of a grid security emergency until blackouts begin; doing so would forego the benefits of issuing preattack emergency orders. It may be possible to develop orders that will offer significant benefits if adversaries strike yet also have little or no impact on normal service—thereby offering “no-regrets” options to employ when the likelihood of an attack remains uncertain. Industry and government partners should also explore options for the preattack phase that would be more disruptive but also offer potentially far-reaching benefits. These two options occupy the left-hand column in Figure 5.

Conservative operations that utilities employ against natural hazards provide a model for protecting the grid in ambiguous preattack situations. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects and prepare for possible response and restoration operations if grid infrastructure is damaged.<sup>120</sup> For

<sup>120</sup> Conservative operations are not defined in the NERC glossary of terms. However, many reliability coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken to “implement



example, reliability coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.<sup>121</sup> Power companies may also cancel noncritical generation and transmission maintenance activities; reduce transfer limits to give the transmission system extra “slack”; and staff their backup control centers, critical BPS substations, and other vital facilities to set the stage for emergency operations as hurricanes approach.<sup>122</sup>

A defining feature of these frequently used conservative operations is that they do not disrupt normal service to customers. Their negligible service impact makes them more viable to implement when the storm’s path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the US coast. Instead, they provide a wide “cone of uncertainty” that becomes increasingly narrow as the hurricane approaches. Utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other conservative operations. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these operations do not affect normal service to customers enhances the willingness of utility leaders to order their implementation while the storm track remains uncertain.

---

additional actions to ensure the BES remains reliable in the face of the additional threats” when “events, conditions, or circumstances may put the Bulk Electric System (BES) at an increased level of risk, compared to normal operating conditions.” See PJM, “Conservative Operations,” 3. Similarly, the Western Electricity Coordinating Council, defines conservative systems operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets “are restricted and managed in order to maintain or restore reliability of the power system from the negative influence of a triggering event or condition.” See Western Electricity Coordinating Council, “Conservative System Operations,” 4.

<sup>121</sup> PJM, “Conservative Operations,” 3.

<sup>122</sup> PJM, “Conservative Operations,” 9.

Industry and government partners should borrow from this model to develop orders for preattack conservative operations against cyber and/or physical attacks. Some have already begun to do so. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting conservative operations to meet the specialized challenges posed by cyber and physical threats.<sup>123</sup> This preparation will be extremely helpful as potential attacks loom. As a regional confrontation or other precipitating crisis intensifies, it is conceivable that the US intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. However, it is much more likely that ambiguities will persist about whether the adversary will actually attack and risk a devastating US response. To ensure that sufficient time is available to implement conservative operations, the secretary may need to order the initiation of such measures when enemy intentions remain uncertain—and when warning indicators may turn out to be false.

Many of the conservative operations that will bolster resilience against adversary attacks would be similar to those developed for natural hazards. For example, preattack emergency orders might direct BPS entities to increase generation reserves and/or re-dispatch resources out of least-cost operations. Other orders might be threat specific: for example, to intensify scrutiny of operational technology networks for malware and implement government-vetted countermeasures in ways that give utilities sufficient latitude to account for their unique system characteristics.

The common denominator for all such options: if the secretary issues orders for BPS entities to adopt conservative operations and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented the orders.

---

<sup>123</sup> See, for example, PJM, *PJM Manual* 13, 73; Lucas, “Conservative Operations”; and SERC, *Conservative Operations Guidelines*.

However, because so many utilities already have robust plans and capabilities to protect their systems from imminent threats, close government–industry coordination will be required to ensure that emergency orders actually assist grid defense rather than function as speed bumps or useless distractions. Reliability coordinators and other grid operators serve as the pointy end of the spear for protecting grid reliability. Mandatory NERC standards require BPS entities to maintain voltage stability, automatic load shedding schemes, and contingency reserves for disturbances.<sup>124</sup> NERC standards also require transmission operators to “develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area.”<sup>125</sup> Balancing authorities have similar requirements to manage generating and demand-side resources in their service areas.<sup>126</sup> These plans are exercised, tested, and frequently updated to bolster their effectiveness for actual emergencies. While many of NERC’s mandatory standards apply when disturbances begin to occur, BPS entities are spring-loaded to implement conservative operations the moment potential hazards begin to emerge.

If major grid disruptions occur, BPS entities will not sit on their hands and wait for the president to declare a grid security emergency and the secretary to issue emergency orders. Indeed, DOE does not contemplate that they will. In the final grid security emergency rule, the department states that the declaration of a grid security emergency “does not preclude electric utilities from taking time-sensitive action to secure the safety, security, or reliability of the electric grid prior to the issuance of an emergency order.”<sup>127</sup>

DOE and its partners can design emergency orders to help supplement and support such industry-led operations. For example, government agencies may acquire highly classified indicators that an attack is imminent. Declaring a grid security emergency and issuing emergency orders for conservative operations could ensure that utilities bolster their preparedness against such attacks on a consistent, nationwide basis, including those utilities that had not yet identified a need to act. Orders to help power companies ramp up and target searches for specific types of malware could supplement utilities’ defensive operations as well. The secretary might also issue orders to ensure that such industry operations benefited from the FPA’s regulatory protections and cost-recovery provisions.

### More Disruptive Preattack Options

Many utilities are also prepared to take pre-event emergency measures that will significantly disrupt normal electric service, yet also offer benefits far beyond those that conservative operations can provide. For example, power companies can selectively halt electric service on warning of catastrophic storm surges. If seawater hits systems that are still carrying electricity, transformers and other difficult-to-replace grid components will suffer catastrophic physical damage. In 2012, weather forecasters warned that Superstorm Sandy might produce storm surges that would inundate critical substations and underground electrical equipment in lower Manhattan. Consolidated Edison’s team made the politically difficult decision to prevent such damage by preemptively cutting of power to the area. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.<sup>128</sup> Moreover, Consolidated Edison limited the shutdown’s disruptiveness by notifying customers hours earlier that the utility might halt service and by already having plans in place to prioritize the

<sup>124</sup> See, for example, NERC, *VAR-001-4.2*; NERC, *Standard PRC-006-3*; NERC, *PRC-010-2*; and NERC, *BAL-002-2(i)*.

<sup>125</sup> NERC, *EOP-011-1*, R1.

<sup>126</sup> NERC, *EOP-011-1*, R2.

<sup>127</sup> DOE, “RIN 1901–AB40,” 1177.

<sup>128</sup> Miller, “Con Edison Shuts off Power.”

restoration of service to hospitals, water-pumping stations, and other critical facilities.<sup>129</sup>

BPS entities continue to use “shutdown on warning” as an effective tool to avoid equipment damage against severe weather and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent equipment damage and speed up restoration. Generation owners similarly chose to shut down or evacuate some generating units in the storm’s projected path.<sup>130</sup>

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and heating and air conditioning systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

DOE and its electricity subsector partners should consider developing emergency orders that offer a similar set of risks and rewards. However, doing so will entail problems beyond those associated with protecting the grid against natural hazards. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an adversary will actually pull the (cyber) trigger and whether attacks are likely to cause demonstrable harm to the US economy, national security, or public health and safety. Measures developed for natural hazards may also offer uncertain benefits against imminent cyber and physical attacks. For example, further analysis will be required to determine whether and how preattack grid shutdowns might help counter specific cyber threats, including attacks that disable

protection systems to facilitate equipment-damaging power surges.

Other disruptive emergency orders could counter a broader range of threats but entail major (and perhaps insurmountable) problems for nationwide employment. The upper left-hand box in Figure 5 offers a prime example of such options: preplanned power islanding. Microgrids offer the most familiar means of establishing power islands.<sup>131</sup> A growing number of military bases, universities, and major hospitals have sufficient generation and other electric infrastructure on-site so that if adversaries black out the surrounding grid (or pose an imminent danger of doing so), those facilities can separate from the grid and operate independently as power islands.

However, microgrids do not offer “bulletproof” power resilience. Cyber adversaries are sure to treat on-base electric infrastructure, including renewable generation assets, as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas-fired generators, the power they provide is only as resilient as the gas transmission and distribution systems that supply them—and cyber threats to natural gas systems are rapidly escalating.<sup>132</sup> Moreover, building microgrids requires extensive investment in grid infrastructure. Investment demands will be especially heavy if installations want to serve not only the critical loads within their perimeters but also the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to building microgrids, power companies are also analyzing ways to establish emergency power islands with less infrastructure investment. One particular option being explored by GridEx participants is to preplan to establish large

<sup>129</sup> DiSavino and Sheppard, “ConEd Cuts Power.”

<sup>130</sup> NERC, *Hurricane Harvey*, v.

<sup>131</sup> DOE’s definition of microgrids: “A microgrid is a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously.” “The Role of Microgrids,” DOE.

<sup>132</sup> DOE, *Quadrennial Energy Review*, 7-7; and Parfomak, *Pipelines*, 2-3.

power islands by using existing grid infrastructure within their boundaries. Utility personnel have noted that they might be able to use legacy balancing areas as a starting point to establish island boundaries. On warning of an imminent attack or under other extraordinary circumstances, utilities would separate a power island from the surrounding grid and operate independently to serve critical loads within it. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, preplanned islands might become a hedge against cascading failures and uncontrolled separation.

In practice, preplanned islanding will be practical only if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for preplanned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands to enable them to function independently of the grid. Moreover, standing up islands would severely disrupt day-to-day service for noncritical customers and create instabilities for surrounding systems that could produce additional service disruptions. Accordingly, preplanned islanding might be considered a “huge-regrets” emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created.

DOE and its industry partners should also consider developing preattack emergency orders that fall between the two extremes of no-regrets options and highly disruptive measures. For example, to avoid remote execution of destructive malware on utility networks, orders might direct utilities to disconnect their systems from the internet. Utilities could also take additional measures to isolate or compartmentalize all control systems. Implementing these

measures would curtail potential attack vectors, but would do so at a price. Disconnecting from the internet would hobble wholesale market operations, disable email as a basic communications tool, affect an entity’s access to other means of communications (i.e., E-ISAC and DOE portals), impact an entity’s ability to comply with regulatory requirements, and produce other undesirable consequences. Any unexpected challenges in isolating or compartmentalizing the control systems that are critical to the functioning of the grid could also jeopardize normal service. Nevertheless, if industry and its government partners can preplan to anticipate and overcome these challenges, even highly disruptive preattack options may be useful to protect the grid from cascading failures.

## Extraordinary Measures when Attacks Are Occurring

Emergency orders when attacks are underway can help utilities prevent widespread instabilities, cascading failures, and uncontrolled separation. Under the auspices of the ESCC, utilities and their resilience partners are already developing “extraordinary measures” to operate the grid if adversaries disable or corrupt SCADA (supervisory control and data acquisition) systems, state estimators, and other operational technology hardware and software components on which utilities typically rely.<sup>133</sup> For example, the North American Transmission Forum is leading an initiative on supplemental operating strategies to help power companies manually cope with the loss of energy management systems and/or SCADA across a large geographic footprint.<sup>134</sup>

---

<sup>133</sup> These extraordinary measures include resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary backup systems, and development of supplemental operating strategies use in “degraded states.” See “ESCC: Electricity Subsector Coordinating Council,” ESCC.

<sup>134</sup> Galloway, “Advancing Reliability and Resilience of the Grid,” 2.



These industry efforts provide a basis to develop grid security emergency orders for extraordinary measures when attacks are under way. So, too, do existing BPS emergency operating plans, capabilities, and operational requirements to manage the grid instabilities. Options for such orders vary in terms of the disruption they would inflict on normal grid operations.

Figure 5 provides an example of a low-disruption order for this phase: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate needs or for the next day). These entities have taken extensive measures to keep market functions separate from their operational control of the grid. Many entities also have mechanisms in place to operate when markets are temporarily suspended. Over extended periods, however, cyber attacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, undercut the valuation of power companies on Wall Street, and magnify the damage to the US economy that attacks on the grid will create.

Regional transmission organizations are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the transmission operator<sup>135</sup> for the Mid-Atlantic and other US regions, has called for the development of mechanisms to permit “nonmarket” operations in extreme circumstances.<sup>136</sup> A number of options exist to provide for such operations. For example, if the secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell

power at a fixed price predetermined by DOE.<sup>137</sup> Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high-benefit/low-disruption emergency orders, including orders for maximum power generation when attacks are under way, will also fall into this category.<sup>138</sup>

Industry and government partners will also need to develop more disruptive emergency orders that can protect grid reliability in extraordinary circumstances. One option to do so involves operating an area in a generation-deficient state for a prolonged period, supported (when practical) by power imported from neighboring regions. The top center box of Figure 5 provides another prominent example: prioritized manual load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by selectively shedding load and implementing rotating blackouts.<sup>139</sup>

A failure to shed load contributed to the cascading failures in the major 2003 blackout. After-action reports from that event found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission

<sup>135</sup> The NERC glossary defines *transmission operator* as “the entity responsible for the reliability of its ‘local’ transmission system, and that operates or directs the operations of the transmission Facilities.” *Transmission operator area* is defined as “the collection of Transmission assets over which the Transmission Operator is responsible for operating.” See NERC, *Glossary*.

<sup>136</sup> PJM, “Comments and Responses,” 6, 39–40.

<sup>137</sup> Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. PJM, “Comments and Responses,” 39.

<sup>138</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual 13*, 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see MISO, “MISO January 17–18 Maximum Generation Event Overview.”

<sup>139</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 11.



lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. A US–Canada task force found that “timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio.”<sup>140</sup> In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.<sup>141</sup>

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for transmission operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation for building emergency orders to reduce the risk that physical and cyber attacks will create cascading blackouts.

One way to shed load would be to order power companies to execute rotating blackouts. In such controlled outages, grid operators interrupt service on a rotating basis to sequential sets of distribution feeders for limited periods (typically twenty to thirty minutes).<sup>142</sup> Grid operators employed rotating blackouts to help protect grid reliability during the “Big Chill” that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT’s rotating blackouts during the event affected a total of 4.4 million customers.<sup>143</sup> The temporary blackouts were no doubt disruptive. However, by reducing the risk of cascading failures, those

outages offered compelling system-wide benefits for protecting reliability.

But rotating blackouts will not offer the best option for load shedding in all grid security emergencies. In the event of a massively disruptive attack, an emergency order might require utilities to shed load without implementing rotating blackouts, because such rotating outages could introduce unacceptable reliability risks during a chaotic and rapidly changing situation. As an alternative, utilities can implement “brownouts”: that is, conduct voltage reductions to maintain a continual balance between supply and demand within a balancing area.<sup>144</sup> However, brownouts and rotating blackouts share a serious limitation: they affect all customers equally. But not all customers will be equally important in a grid security emergency. DOE and industry will need orders and implementation plans for manual, prioritized load shedding, so utilities can focus on sustaining power flows to hospitals and other critical loads while also reducing the risk of cascading power failures. NERC already requires BPS entities to have plans for both automatic and manual load shedding.<sup>145</sup> Utilities and DOE should use these requirements as the starting point to design emergency orders for extraordinary measures that would supplement what BPS entities are already prepared to do to if major instabilities occur.

## Emergency Orders to Support Power Restoration

The rightmost column in Figure 5 provides the third category for emergency orders: those that can help grid owners and operators restore power after widespread

<sup>140</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 147.

<sup>141</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 77.

<sup>142</sup> NERC, *Reliability Terminology*, 1.

<sup>143</sup> FERC and NERC, *Restoration and Recovery Plans*, 61.

<sup>144</sup> NERC, *Reliability Terminology*.

<sup>145</sup> NERC standards currently emphasize automatic load shedding to protect grid reliability. See NERC, *Standard PRC-006-3*; and NERC, *PRC-010-2*. However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing emergency orders to prevent or mitigate cascading failures. See NERC, *EOP-011-1*.

outages occur. In past cascading failures of the US electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days (and in some cases much less time) because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators, transmission lines, and other system components are designed to trip offline when instabilities occur, thereby protecting them from damaging power surges—and leaving them available to help rapidly reestablish the flow of power.<sup>146</sup> However, if cyber or physical attacks destroy critical system components, requirements to repair or replace such assets could greatly lengthen and complicate the restoration of service. Emergency orders can support restoration operations and better align them with national-level priorities.

Emergency orders for the restoration phase can also account for the risk that adversaries may continue their attacks as power companies begin to restore service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to US military bases and other vital facilities and to seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeting power restoration operations can help adversaries achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply. Risks of reattack should help drive the design of restoration-phase emergency orders.

Advanced persistent threats hidden in utility networks will pose especially significant challenges for restoration. This malware may enable adversaries to conduct recurring attacks based on timing or network

conditions. Unless utilities thoroughly eradicate such malware, repeated outages could impede restoration operations and put the grid at sustained risk of cascading failures.<sup>147</sup> Physical attacks against restoration personnel and replacement equipment in transit would pose additional problems. Grid security emergency orders can help utilities restore electric service even if they remain “under fire” from cyber and kinetic weapons.

Such orders will differ in the degree to which they could alter existing utility plans to restore power. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks, and barges) from where power companies store them to where they are needed as replacements.<sup>148</sup> Subsequent portions of this report examine how DOE could collaborate with other federal agencies and state and local officials to waive transportation regulations and bolster security support for such operations. The secretary could also issue orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, ports, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these prioritized customers. Emergency orders can help incorporate other national security-related assets that utility plans do not typically include, such as components of the defense industrial base essential for resupplying US forces abroad.

DOE and its industry partners should also create template emergency orders for in extremis restoration operations that would more sharply depart from existing industry plans and procedures. The upper right-hand box of Figure 5 offers an example

<sup>146</sup> NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, 1.

<sup>147</sup> Homeland Security Advisory Council, *Final Report*, 7.

<sup>148</sup> DOE, *Strategic Transformer Reserve*, 12–13.

of one such option. If adversaries damage or destroy an extraordinarily large number of transformers, the secretary might order utilities to remove surviving in-service transformers in the same voltage class from their substation and transport them to serve vital national security facilities in the National Capital Region or other areas. Orders of this kind could create severe disruptions in existing service. They might even impede system restoration if utilities and their government partners have not adequately prepared to account for challenges regarding transformers' technical specifications and the BPS's overall configuration. However, if these challenges can be addressed, the benefits might be greater still for helping the United States defeat its adversaries.

Other in extremis orders could help utilities operate the grid if equipment damage is so extensive (or reattacks are so effective) that full system restoration will require many weeks or even months. The FERC/NERC study on severe impact resilience (May 2012) found that coordinated cyber and physical attacks may force the grid into a "new normal" state of "degraded planning and operating conditions" that could last for months or years, including reduced generation and transmission resources and planned and unplanned rotating blackouts.<sup>149</sup> DOE and power companies should consider how emergency orders and supporting regulatory waivers might help electric utilities serve priority loads and accelerate restoration under new normal conditions.

One option to do so is to preplan for the waiver of selected reliability standards. The *Severe Impact Resilience* study recognized that catastrophic events could "put entities in a position where they cannot comply with all standards." However, in part due to the difficulty of predicting the circumstances that entities will face, the study recommended against preplanning for waivers. Instead, the study proposed relying on entities to "do the right thing" for reliability

and public safety" and self-report violations as circumstances permit.<sup>150</sup>

NERC should reconsider this conclusion in light of the secretary's new grid security emergency authorities and the waiver provisions they entail. FERC, NERC, and their industry and government partners should identify specific regulatory waivers and related measures that could provide the basis for utilities' contingency planning for new normal operations.

One such option lies in reliability standards for managing unforeseen contingencies. Currently, NERC standards require BPS entities to operate in an N-1 state: that is, they must be able to sustain service even if they suffer the most severe single contingency (such as the loss of a single critical line, transformer, or generator) possible in their system.<sup>151</sup> Operators may be required to shed load prior to any contingency to maintain the N-1 state. These requirements apply during normal day-to-day operations as well as during system restoration.

Returning to an N-1 state in the face of coordinated cyber and physical attacks is likely to be a lengthy process involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. To help enable utilities to serve critical facilities during such sustained events, the secretary might issue emergency orders that explicitly allow utilities to function in an N-0 operating state (as long as doing so did not risk causing cascading failures or equipment damage).<sup>152</sup>

Issuing such orders could entail important benefits. Operating at N-0 would give utilities greater operating flexibility and ensure that entities can continue to serve as much load as possible during a grid security

<sup>149</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

<sup>150</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 17.

<sup>151</sup> NERC, *BAL-002-2(i)*, requirement R2; NERC, *TOP-001-3*, R12 and R14; and NERC, *IRO-008-2*, R5 and R6.

<sup>152</sup> For N-0, all elements must be within thermal and voltage limits prior to any contingency.

emergency, including military installations and other priority customers. Unlike under N-1 operations, entities would be required to shed load only prior to any contingency for the most severe single contingencies if any of those single contingencies would cause cascading failures, or after a contingency that required load shedding to eliminate overloads or low voltage.

But operating at N-0 would also entail significant risks. N-1 standards exist for compelling reasons: they help protect grid reliability against severe contingencies. Deviating from N-1 requirements will create greater risks of causing further blackouts in new normal conditions. Moreover, N-0 operations would require even greater coordination among BPS entities (including reliability coordinators, transmission owners, and local control centers), as a single outage could result in equipment overloads or voltage violations and require extraordinary mitigation measures. Accordingly, this option will be feasible only if DOE partners with FERC, NERC, and entities to fully understand and mitigate such risks, as well as maximize the potential benefits of N-0 operations for serving critical national security-related loads.

## Additional Emergency Order Design Parameters and Supporting Initiatives

Adversaries will attempt to black out the US grid to achieve their broader political, economic, and military objectives in a conflict. Government agencies and the electricity subsector should design emergency orders to help prevent attackers from accomplishing their objectives, and—ideally—to help deter them from attacking at all.

However, deterring and defeating attacks on the grid will require resilience improvements beyond the electricity subsector. Attackers may simultaneously strike electric and communications systems to both disrupt the grid and impede the issuance and

implementation of emergency orders. Adversaries may also seek to incite public panic through social media and other information warfare operations to advance their broader political objectives. Countering such efforts will require unprecedented collaboration among utilities, government agencies, media, and the broader telecommunications sector.

Designing and implementing emergency orders to blunt attacks by Russia, China, and other potential high-capability adversaries will place extraordinary burdens on electric utilities—burdens that few ratepayers and utility investors will be eager to bear on their own. To help power companies meet these challenges, it will be essential to fully leverage the regulatory waiver and cost-recovery provisions of the FPA, and examine whether Congress should expand these provisions as threats continue to intensify.

## Deterring and Defeating US Adversaries

The US *National Security Strategy* emphasizes that cyber threats to US critical infrastructure are becoming increasingly severe. In particular, the strategy notes that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>153</sup> Pairing cyber attacks with coordinated physical strikes against transformers and other critical grid infrastructure would exacerbate these disruptive effects.

The strategy identifies two primary means for deterring catastrophic attacks, both of which can be supported by emergency orders and implementation plans:

- (1) Convince adversaries that they will suffer “swift and costly consequences” if they strike the grid or other US targets, and that the United States “can and will defeat them” if deterrence fails.<sup>154</sup>

<sup>153</sup> White House, *National Security Strategy*, 13, 28.

<sup>154</sup> White House, *National Security Strategy*, 28.



- (2) Strengthen infrastructure resilience to create “doubt in our adversaries that they can achieve their objectives” if they do attack (i.e., deterrence by denial).<sup>155</sup>

### **Deterrence through Cost Imposition: Protecting Defense Critical Electric Infrastructure**

In amending the FPA, Congress placed a particular emphasis on the need to protect the reliability of defense critical electric infrastructure (i.e., grid components that serve military bases and other facilities “critical to the defense of the United States” and vulnerable to the disruption of grid-provided electricity).<sup>156</sup> Emergency orders to protect such infrastructure can help ensure that US bases have the power they need to respond to attackers. But prioritizing defense installations for support in grid security emergencies will require deeper analysis of US deterrence requirements, given DOD’s growing dependence on civilian assets and functions to execute defense missions. Deterrence by cost imposition will also depend on convincing potential adversaries that the United States will be able to identify them as the perpetrators of attacks on the grid. DOE and its industry partners should explore how emergency orders can facilitate attack attribution, as well as provide broader support for the credibility of the US deterrence posture.

A relatively small number of military bases are responsible for inflicting unacceptable costs on potential adversaries. The US Defense Science

Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of US strike systems (cyber, nuclear, and nonnuclear) and supporting infrastructure to ensure “that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks.”<sup>157</sup> Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which US strike systems rely and ensure that they have reliable power even in extended conflicts.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The strategy emphasizes that “we must convince adversaries that we can and will defeat them—not just punish them if they attack the United States.”<sup>158</sup> Defeating adversaries in regional contingencies in the South China Sea, the Baltics, or other potential conflict zones will place special burdens on US grid resilience. US capabilities to conduct operations abroad are increasingly dependent on domestic military and civilian assets. In particular, a vast array of US defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy, operate, and sustain US power projection forces for regional conflicts.

This dependence makes the grid a prime target for attack. The DOD *Mission Assurance Strategy* notes that adversaries may seek to disrupt power projection capabilities by attacking the domestic infrastructure systems on which they depend. In particular, the strategy warns that “potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting

<sup>155</sup> White House, *National Security Strategy*, 13, 28. The literature on security studies defines deterrence by denial in a variety of ways. This report follows the definition used in the *National Security Strategy*, which is consistent with the definition employed in the Obama administration’s deterrence policies. See Lynn, “Defending a New Domain.” For broader studies of deterrence by denial, and critiques of the way in which the strategy employs the term, see Fischerkeller and Harknett, “Deterrence Is Not a Credible Strategy”; Mitchell, “Case for Deterrence by Denial”; Gerson, “Conventional Deterrence,” 40; and Nye, “Deterrence and Dissuasion,” 56–58.

<sup>156</sup> 16 U.S.C. § 824o–1, (a)(4).

<sup>157</sup> Miller and Gosler, “Memorandum.” See also pp. 3, 6–7, 11–12, and 17–18 of the report.

<sup>158</sup> White House, *National Security Strategy*, 28.



critical defense and supporting civilian capabilities and assets,” including the US power grid.<sup>159</sup>

Ensuring the availability of resilient power for ports and other civilian assets essential for power projection will require emergency orders to serve an expanded set of customers, far beyond those responsible for strike operations. These orders will also need to encompass a much larger array of defense critical electric infrastructure owners and operators.

Electric companies and defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds from separate high-voltage transmission substations to serve defense installations provides a valuable means of strengthening resilience against physical attacks.<sup>160</sup> Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.<sup>161</sup> Utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as power islands independent of the surrounding grid.<sup>162</sup>

While valuable, these initiatives do not eliminate the need to develop national defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases and will not necessarily provide resilience against cyber attacks (since even redundant feeds may share common cyber vulnerabilities). Emergency generators will break down in long-duration outages. Moreover, resupplying them with fuel will become increasingly difficult at installations that lack massive storage

tanks. Large-scale microgrids for islanded operations can provide more resilient power. DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction and scale them to serve infrastructure loads outside the base that are essential for on-base operations. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for war fighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, including the intermodal transportation systems that help deploy and sustain US forces abroad.

DOE and its industry partners can design emergency orders to support US deterrence credibility and power projection capabilities far more quickly and with less infrastructure investment. However, for utilities to implement these orders, they must first know which customers are of the highest priority for sustaining and restoring service when enemies strike. Section 215A of the FPA provides the ideal starting point develop and share such data. The act requires the secretary of energy, in consultation with other federal agencies and grid owners and operators, to identify and designate “critical defense facilities” in the forty-eight contiguous states and the District of Columbia that are “(1) critical to the defense of the United States; and (2) vulnerable to a disruption of electric energy provided to such facility by an external provider.”<sup>163</sup> Congress’s definition of defense critical electric infrastructure also helps guide implementation of that requirement. Such assets include “any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]” as a critical defense facility, “but is not owned or operated by the owner or operator of such facility.”<sup>164</sup>

<sup>159</sup> DOD, *Mission Assurance Strategy*, 1.

<sup>160</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39.

<sup>161</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 40.

<sup>162</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39. See also Van Broekhoven et al., *Microgrid Study*; and Marqusee, Schultz, and Robyn, *Power Begins at Home*, 13–15. A number of “islandable” microgrid projects are under way at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See McGhee, “EEI Executive Advisory Committee,” 4; and Kaften, “DoD Tests Energy Continuity.”

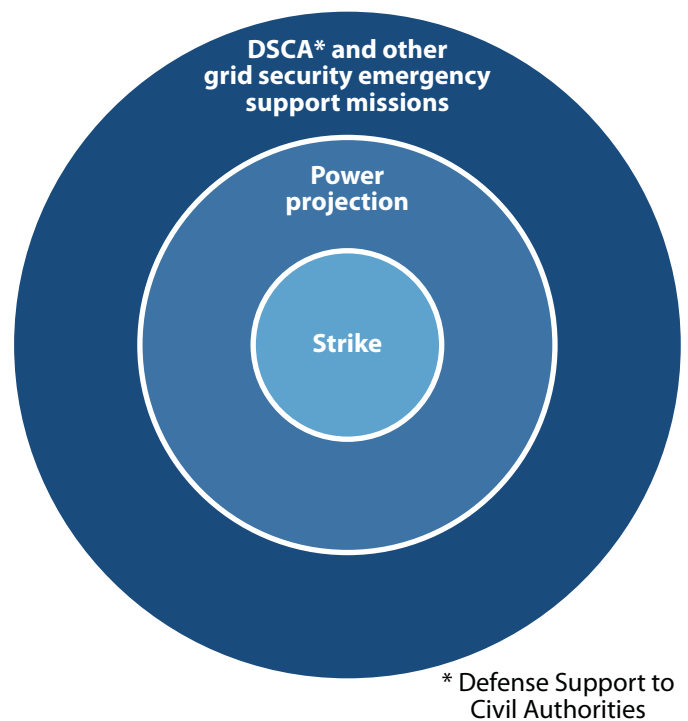
<sup>163</sup> 16 U.S.C. § 824o–1, (c).

<sup>164</sup> 16 U.S.C. § 824o–1, (a)(4).

DOE is already working with DOD to identify defense critical electric infrastructure and the installations this infrastructure serves. DOD has a well-established, continuously updated list of critical military bases and other DOD assets to support this identification process.<sup>165</sup> However, deterrence and power projection will also depend on sustaining electric service to a diverse array of ports, transportation systems, and other civilian-owned infrastructure. Figure 6 illustrates how DOE, DOD, and their partners might categorize all such defense-related assets and the defense critical electric infrastructure that grid security emergency orders should help protect.

At the innermost core lie those installations and supporting infrastructure capable of inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital. Protecting the reliability of the defense critical electric infrastructure on which they depend should be the top nationwide priority for developing emergency orders and company-specific implementation plans.

The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining these assets abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the US grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. DOD is in the process of identifying the specific facilities and supporting infrastructure that are required to help execute operational plans around the globe.<sup>166</sup> The department also has well-established criteria and assessment methods to prioritize these supporting assets for risk mitigation.<sup>167</sup> DOD and DOE should use these tools to identify the broader set of defense critical electric infrastructure needed for deterrence



**Figure 6. Categories for Protecting Defense Critical Electric Infrastructure**

and to help power companies preplan to support critical assets within their service footprints.

The third circle includes the still larger array of defense installations, including National Guard bases, which would be essential for providing defense support to civil authorities if disruptions of the grid jeopardize public health and safety.<sup>168</sup> During Hurricane Maria (2017), Superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, lodging, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and delivering other assistance. Protecting or rapidly restoring the reliability of the defense critical electric infrastructure that supports

<sup>165</sup> See DOD, *Manual 3020.45*; and DOD, *Directive 3020.40*.

<sup>166</sup> DOD, *Directive 3020.40*.

<sup>167</sup> DOD, *Manual 3020.45*.

<sup>168</sup> Of course, many National Guard installations that could conduct defense support operations may also be responsible for assisting war fighting operations abroad, and would therefore fall within the second circle as well.

these defense-support-to-civil-authorities functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public.<sup>169</sup>

Building preparedness for grid security emergencies can also help meet an underlying challenge for deterrence: attack attribution. To convince foreign leaders that they will suffer swift and costly consequences if they strike the grid, those leaders must first believe that the United States will be able to identify them as the attackers.<sup>170</sup> The Federal Bureau of Investigation (FBI) and other federal agencies are improving their attribution capabilities.<sup>171</sup> US agencies also devote massive resources to human and technical intelligence collection on potential adversaries, which could further assist attack attribution.<sup>172</sup> Nevertheless, adversaries may seek to strike in ways that complicate attack forensics by employing wiper tools and using other tactics, techniques, and procedures to cover their tracks.<sup>173</sup>

Emergency orders can help defeat adversaries' efforts to evade attribution. By refining the FPA's information sharing mechanisms and building them into emergency orders, utilities and their government partners can strengthen their ability to share malware samples and other information on threat signatures.<sup>174</sup> New technologies can bolster such collaboration. For

example, the Containerized Application Security for Industrial Control Systems project is designed to help grid operators isolate and capture malware on their systems, enabling samples to be shared with government agencies while still preventing that malware from disrupting system operations.<sup>175</sup>

Developing emergency orders and implementation plans to defend the grid can also provide broader support for attribution. James Miller notes that "while cyber hardening of US critical infrastructure will never be good enough to prevent a Russia or China from being able to threaten a major attack, it can cause them to have to be 'noisier' to do so, thereby boosting our confidence in attribution."<sup>176</sup> Emergency measures to protect grid reliability can complicate attack planning and, ideally, drive adversaries to strike in ways that will make them easier to identify.

### **Deterrence by Denial: Protecting Critical Electric Infrastructure**

Convincing adversaries that they will suffer unacceptable costs if they strike the grid is only one means of deterring such attacks. Another means is to reduce the benefits that adversaries expect to achieve by attacking. In classical deterrence theory, both factors combine to influence an adversary's decision on whether to strike. As Joseph Nye Jr. puts it, "deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."<sup>177</sup>

The *National Security Strategy* calls for measures that can prevent attackers from achieving the goals they seek and thereby strengthen deterrence by denial. The strategy states that "we must ensure the ability to deter enemies by denial, convincing them that they cannot accomplish their objectives through the use of

<sup>169</sup> Countering such adversary efforts will also require protecting electric service to financial institutions, regional hospitals, and other civilian assets essential to the US economy and public health and safety. The next section of the report examines these requirements and their implications for deterrence and emergency order design.

<sup>170</sup> On the tasks that attribution comprises, see Lin, "Escalation Dynamics," 49–50.

<sup>171</sup> Smith, "Roles and Responsibilities." See also Newman, "Hacker Lexicon."

<sup>172</sup> Miller, "Cyber Deterrence."

<sup>173</sup> Newman, "Hacker Lexicon."

<sup>174</sup> See 16 U.S.C. § 824a–1, (d). Later sections of this report provide a more detailed assessment of provisions for improved information sharing.

<sup>175</sup> "Sandia's Grid Modernization Program Newsletter," Sandia National Laboratories.

<sup>176</sup> Miller, "Cyber Deterrence."

<sup>177</sup> Nye, "Deterrence and Dissuasion," 45.

force or other forms of aggression.”<sup>178</sup> Ensuring that the grid and other infrastructure sectors can survive attacks and rapidly recover from service interruptions plays an especially important role in the administration’s deterrence posture. The strategy notes that “a stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.”<sup>179</sup> More recent statements of administration policy also note that deterrence by denial “must be foundational to the U.S. deterrence approach,” and that US efforts must continue “to deny adversaries the benefits of their malicious cyber activities.”<sup>180</sup>

Emergency orders and implementation plans may be able reduce the benefits that adversaries expect to achieve by attacking the grid. Preattack orders to bolster grid defenses can impede adversary efforts to disrupt grid reliability. Once attacks are under way, orders for prioritized load shedding and other extraordinary measures can help limit the damage the adversaries may hope to inflict on financial institutions, hospitals, and other electricity-dependent facilities. Orders that accelerate power restoration to these critical facilities may also reduce the effects of an attack, and thereby strengthen deterrence by denial.

The FPA is ready-made to support such improvements. In addition to protecting defense critical electric infrastructure, and thereby assisting deterrence through cost imposition, the act also authorizes orders to protect a much broader portion of the grid: critical electric infrastructure. Such infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>181</sup> Orders to help utilities defend critical electric infrastructure can reinforce deterrence by denial—and, if deter-

rence fails, reduce the devastation that adversaries will create.

However, developing and implementing such orders will entail major challenges. Some deterrence theorists doubt whether deterrence by denial is practical in cyberspace, in part because offensive capabilities are so much stronger than cyber defenses. The conclusion of this report will examine those arguments and explore broader opportunities to bolster deterrence and help the United States defeat our adversaries if conflicts nevertheless occur. First, however, DOE and its partners will need to overcome two impediments to protecting critical electric infrastructure: determining which specific facilities and functions are truly critical, and securely sharing that information with utilities so they can refine their operational plans for grid security emergencies.

### **Building a “Section 9+ List:” Prioritizing Infrastructure for Sustainment and Restoration**

Identifying and prioritizing critical electric infrastructure will be far more difficult than doing so for defense critical electric infrastructure. If adversaries create cascading blackouts across one or more interconnections, the disruption of many thousands of civilian-owned facilities could negatively affect national security, the US economy, and public health and safety. Utilities cannot possibly prioritize the flow of power to all such facilities. Government agencies and their private sector partners will need to determine which specific customers (and the critical electric infrastructure that serves them) are most vital to the nation and must continue to receive power if widespread instabilities occur.

Executive Order 13636 (February 2013) provides an existing methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the secretary of homeland security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security,

<sup>178</sup> White House, *National Security Strategy*, 28.

<sup>179</sup> White House, *National Security Strategy*, 13.

<sup>180</sup> DOS, *Recommendations*, 2.

<sup>181</sup> 16 U.S.C. § 824o–1, (a)(2).



or national security.”<sup>182</sup> That standard—catastrophic damage—provides a useful criterion to identify the highest-priority assets and associated critical electric infrastructure for protection by emergency orders in grid security emergencies. Over time, orders and contingency plans could gradually encompass less-critical facilities and grid infrastructure.

Of course, the section 9 methodology and subsequent list were never intended to support the implementation of section 215A of the FPA. As a result, the section 9 methodology falls short of meeting all the requirements for supporting emergency order design. One gap lies in the threats that drive the selection of critical assets. Section 9 focuses exclusively on infrastructure at risk from cyber attacks. The FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on electric systems. Executive Order 13636’s section 9 requirements also create a “corporate”-level list that is not broken down into the key assets within those corporations (i.e., facilities, systems, and nodes). More fine-grained data and analysis will be required to identify facilities for which sustained electric service will be most crucial. Efforts to prioritize grid service will also need to account for the increasingly complex interdependencies between US infrastructure sectors.<sup>183</sup>

Despite these shortfalls, Executive Order 13636’s methodology can provide a valuable starting point for identifying the most vital critical electric infrastructure and supporting assets. DOE and its industry partners should leverage that methodology to create a “section 9+” list, tailored to fulfill FPA emergency order requirements. Other government initiatives to prioritize critical infrastructure could

also make valuable contributions to the list and overall prioritization effort. For example, DHS’s May 2018 cyber strategy emphasizes the importance of “identifying the most critical [federal] systems and prioritizing protections around those systems.”<sup>184</sup> A number of other initiatives could provide significant value as well.<sup>185</sup> Building a section 9+ list would also benefit from the inclusion of input from cleared state regulators and homeland security and emergency management officials.

DHS’s National Risk Management Center can help integrate these sources of data and develop a comprehensive, cross-sector basis for prioritizing the sustainment and restoration of power to critical facilities. Government agencies within the center will collaborate with the private sector to “identify, assess, and prioritize efforts to reduce risks to national critical functions, which enable national and economic security.” One immediate task will be to “help define what is truly critical.”<sup>186</sup> As this work

<sup>184</sup> DHS, *Cybersecurity Strategy*, 8.

<sup>185</sup> There are numerous programs that DOE and its partners could leverage to build the section 9+ list. DHS’s National Critical Infrastructure Prioritization Program aims to identify “nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance.” See DHS, *NIPP 2013*, 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on “lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity” (p. 24). Despite its focus on terrorist threats, *Homeland Security Presidential Directive 7* also requires the secretary of homeland security to identify and prioritize systems and assets that, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the “loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States” and lower jurisdictions. The national-level priorities on this list could also be helpful. 6 U.S.C. § 124l, (a)(2).

<sup>186</sup> “National Risk Management Center Fact Sheet,” DHS.

<sup>182</sup> Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*.

<sup>183</sup> For methodologies and data-gathering strategies to assess cross-sector interdependencies, see EIS Council, *E-PRO Handbook III*; and Homeland Security Advisory Council, *Final Report*.



goes forward, the center's efforts could contribute to the development of a section 9+ list that will be essential for grid security emergency preparedness.

### **Sharing the Section 9+ List and Protecting Critical Electric Infrastructure Information**

In addition to identifying assets most in need of power, it will also be essential to share that data with the utilities responsible for providing prioritized service. Current section 9 guidance lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the federal government tells grid owners and operators if they are on the section 9 list, it rarely informs them about the section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own system configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data with government partners. Public sector leaders will need to reinforce their industry counterparts' confidence that government agencies will not use company-provided information for regulatory compliance, antitrust, or other purposes not explicitly approved through industry-government dialogue.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that critical companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations or supply chains in one industry can produce unintended and unforeseen effects on overall system resilience. Private

companies will need to help government agencies modify the section 9+ list as they reconfigure their operations and create new dependencies on outside service and product providers.

Securing and limiting the distribution of this classified data will also be a prerequisite for countering potential attacks. If adversaries acquired the section 9+ list, it would provide a roadmap that they could use to maximize their devastation of US critical infrastructure. However, measures to protect this data must be complemented by improved mechanisms to provide sensitive information to industry personnel who have the requisite security clearances.

Section 215A of the FPA offers a starting point to meet these requirements. The FPA provides for the sharing of critical electric infrastructure information, defined as information generated by FERC or other federal agencies related to identified (or proposed) critical electric infrastructure "that is designated as critical electric infrastructure information by the Commission or the Secretary" or that qualifies under FERC's critical energy infrastructure information scheme.<sup>187</sup> The FAST Act amendments directed FERC to facilitate the voluntary sharing of such information "with, between, and by" BPS entities and their government partners.<sup>188</sup> The amendments also require FERC to create criteria and procedures to designate certain information as critical and prohibit unauthorized disclosure of that information.<sup>189</sup> To help meet these requirements, FERC incorporated and is building on its well-established mechanisms to protect critical energy infrastructure information.<sup>190</sup>

---

<sup>187</sup> The definition excludes classified national security information. 16 U.S.C. § 824o-1, (a)(3).

<sup>188</sup> This includes NERC, the E-ISAC, regional entities, and "other entities determined appropriate by the Commission." See 16 U.S.C. § 824o-1, (d)(2)(D).

<sup>189</sup> 16 U.S.C. § 824o-1, (d)(2).

<sup>190</sup> FERC, *Regulations Implementing FAST Act Section 61003* (Order No. 833), 157 FERC ¶ 61,123, 13. See also FERC,

Other initiatives are also under way to provide for the protected data sharing essential for preplanning grid security emergency operations. DOE is working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate assets identified as defense critical electric infrastructure. Going forward, DOE, FERC, and their industry partners should refine their equivalent mechanisms to securely distribute data on critical electric infrastructure and the water systems, communications centers, and other essential non-defense assets that must continue to function in grid security emergencies.

## Communications Requirements for Issuing and Employing Emergency Orders

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phones and other normal means of communication fail. These systems often provide connectivity with neighboring BPS entities and, to an increasing extent, entities that are farther away. Under the ESCC, industry has also built an extensive set of playbooks to help companies decide what to tell customers about an incident and to unify messaging between government officials and industry representatives on estimated times of restoration and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. Preparedness for grid security emergencies will require additional progress in four areas: (1) refining consultative mechanisms and protocols for the sequential (though potentially overlapping) phases of such emergencies; (2) ensuring that communications

systems can survive adversaries' attacks; (3) authenticating emergency orders and protecting the security of sensitive data; and (4) determining what to say to the US public and accounting for the risk that adversaries will conduct information warfare operations to intensify panic and incite disorder.

## Initial Consultations and Sustained Communications

As with the phases of grid security emergency declarations, the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Preattack consultations constitute the initial stage. As noted above, the FPA specifies that before the secretary issues emergency orders, DOE will consult with power companies and other BPS stakeholders "to the extent practicable . . . regarding implementation of such emergency measures."<sup>191</sup> This report recommends that federal officials also consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The grid security emergency rule clarifies how DOE's Office of Electricity Delivery and Energy Reliability will consult on emergency orders.<sup>192</sup> The rule states that, if practicable, the E-ISAC is one of the organizations the secretary will consult. Such consultations will be particularly useful for sharing data (including classified data) on attacks that are imminent or under way. The rule also notes that DOE will consult with the ESCC. The ESCC will provide an especially valuable source of industry perspectives on grid security emergency declarations and emergency orders because it represents all components of the electricity subsector and has extensive experience in coordinating the industry's incident response operations. In addition, the rule states that "efforts

*Regulations Implementing FAST Act Section 61003* (Order No. 833-A), 163 FERC ¶ 61,125; and 18 CFR 388.113.

<sup>191</sup> DOE, "RIN 1901-AB40," 1774.

<sup>192</sup> DOE, "RIN 1901-AB40," 1181.

will be made” to consult with NERC, regional entities, “owners, users, or operators” of critical and defense critical electric infrastructure (including regional transmission operators), appropriate federal and state agencies, and other grid reliability stakeholders.

Issuing emergency orders constitutes the second stage. DOE’s grid security emergency rule states that the department will “communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances.”<sup>193</sup> The E-ISAC will likely play a critical role in such communications, since it maintains a detailed, continuously updated list of all BPS owners, operators, and registered users (distribution entities). DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.<sup>194</sup> As long as these mechanisms can be hardened as necessary to survive adversaries’ attacks, leveraging them for grid security emergencies will be much more efficient than creating a separate, unfamiliar system for communicating emergency orders.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders. Attacks on the grid are unlikely to be “one and done.” As adversaries continue to try to destabilize the grid, and power companies respond with emergency operations to protect and restore electric system reliability, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional orders and response activities—potentially on a nationwide basis.

Reliability coordinators will be a critical touchpoint between DOE and individual BPS entities, serving as a focal point between DOE (and other government

leaders) and the power companies that are in their purview. This positioning makes them well suited to communicate secretary-issued orders to individual utilities. Moreover, given reliability coordinators’ responsibilities and authorities to help maintain grid reliability when incidents occur, they will also be ideally positioned to understand how grid security emergency orders should supplement BPS emergency operations that are already under way.

Sustained communications will also be necessary to meet an additional FPA requirement: responding to DOE requests for information on the implementation of emergency orders. The grid security emergency rule specifies that “beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order.”<sup>195</sup> Sustained communications links between DOE and BPS entities will be required to meet such requests for information. However, beyond compliance issues, continuous communications will also be required as government and industry partners assess the effectiveness of emergency operations and identify requirements for additional actions.

### Survivability of Communications

Adversaries will have compelling incentives to combine attacks on the grid with strikes against US communications systems. The 2015 attack on Ukraine’s electric grid illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone networks; the latter attack prevented customers from reporting outages and disrupted grid operators’ ability to conduct restoration operations.<sup>196</sup> In turn, if adversaries can lengthen power outages by disrupting communications systems essential

<sup>193</sup> DOE, “RIN 1901-AB40,” 1181.

<sup>194</sup> DOE, “RIN 1901-AB40,” 1177.

<sup>195</sup> DOE, “RIN 1901-AB40,” 1182.

<sup>196</sup> “Alert (IR-ALERT-H-16-056-01).”

for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications-system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually reinforcing disruptions in both sectors.

We should assume that adversaries will design their attacks to maximize multisector failures, especially since they would already be facing the risk of US response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry–government coordination in grid security emergencies. Enemies might strike communications systems to hobble efforts to share preattack threat data and convey emergency orders. Once attacks on the grid were under way, adversaries could also seek to cripple the communications systems needed to coordinate emergency operations and assess requirements for additional measures.

Strengthening the survivability of existing communications links will be essential to manage these risks. To date, ESCC consultation and coordination mechanisms have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to distributed denial-of-service attacks and a range of other increasingly severe threats,<sup>197</sup> as well to the loss of the grid-provided electricity on which many such systems depend (especially in long-duration outages that put emergency power assets at risk).

Adversaries may also seek to disrupt systems essential for information sharing. For example, the Cybersecurity Risk Information Sharing Program and other E-ISAC notification procedures and portals are in place to alert utilities when adversaries

are implanting malware on critical systems.<sup>198</sup> This includes the E-ISAC's new Critical Broadcast Program, which is intended to operationalize the organization's information sharing capabilities.<sup>199</sup> The FBI and DHS also issue alerts to the energy sector, as in the case of CrashOverride.<sup>200</sup> However, many of these warning and information sharing mechanisms rely on the internet or other potentially vulnerable systems. Industry and government should explore options to ensure that they can still convey essential data in the face of sophisticated attacks on the communications sector.

In addition, adversaries may seek to disrupt the issuance of emergency orders. DOE's grid security emergency rule notes that the department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include "essential actions" to protect BPS reliability, which require recipients to respond as defined in the alert.<sup>201</sup> DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across registered entities. NERC already distributes alerts broadly to BPS users, owners, and operators in North America. Hence, the alert system provides DOE with an opportunity for "one-stop shopping" when issuing emergency orders. The secretary could issue an order to NERC for distribution to both regional operating organizations (regional transmission organizations, independent

<sup>197</sup> Banham, "DDoS Attacks."

<sup>198</sup> "Energy Sector Cybersecurity Preparedness," DOE; and "Electricity Information Sharing and Analysis Center," NERC.

<sup>199</sup> The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See Lawrence, de Seibert, and Daigle, "E-ISAC Update."

<sup>200</sup> "Alert (TA17-163A)."

<sup>201</sup> "About Alerts," NERC.



system operators, reliability coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is email based.<sup>202</sup> As such, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also includes only those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for implementing emergency orders for prioritized load shedding and other actions to sustain power to critical facilities.

Moreover, while the NERC alert system could provide a means of communications across BPS users, owners, and operators, NERC primarily uses the system to communicate alerts of voluntary actions to be taken by electric industry stakeholders. Using the NERC alert system to instead communicate a mandatory action pursuant to a DOE emergency order would require clear coordination and communication to ensure that the order and associated requirements for action are fully understood. In addition, while the NERC alert system offers a proven means to convey unclassified information, the system may not be well suited to distribute classified data.

To fill these gaps, industry and government partners should consider measures to bolster the NERC alert system or create fallback options for survivable communications. Satellite phones offer a prominent option for operational coordination. These phones are widely deployed both among BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies.

Retired US Air Force General William Shelton, who directed the US Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community."<sup>203</sup>

Accordingly, power companies are ramping up their investments in terrestrial emergency communications systems that are hardened against cyber and physical attacks and can be used to sustain critical grid functions even if satellite phones fail.<sup>204</sup> Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are under way to build dark fiber or other survivable links between BPS entities—much less between those entities and DOE. The National Infrastructure Advisory Council study *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish "separate, secure communications networks specifically designated for the most critical cyber networks, including 'dark fiber' networks for critical control system traffic and reserved spectrum for backup communications during emergencies."<sup>205</sup>

The council's study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. In doing so, DOE should leverage lessons learned from the communications sector and specifically from the National

<sup>202</sup> "About Alerts," NERC.

<sup>203</sup> Shelton, "Threats to Space Assets," 3.

<sup>204</sup> FERC and NERC, *PRASE*, 15.

<sup>205</sup> NIAC, *Securing Cyber Assets*, 7.



Security Telecommunications Advisory Committee, which has extensive experience in building redundant and survivable systems.<sup>206</sup> However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities “can communicate with utility crews working in the field to manually restore power” and conduct other postattack operations.<sup>207</sup> Survivable communications systems must also be able to coordinate emergency operations across the electricity subsector and with supporting government agencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when those orders are needed most.

### Authenticating and Securing Emergency Orders

In addition to disrupting the availability of communications systems, adversaries may also seek to corrupt the content of emergency orders and coordination messages, and gain access to classified US data to help defeat grid protection measures. One near-term requirement will be to ensure that utilities can authenticate the orders they receive from DOE. Power companies will need to be able to verify that an order has actually come from the secretary, and that adversaries have not altered its content. Verifying the authenticity of orders will be especially important if such orders require extraordinary measures that could further disrupt normal service and affect public health and safety.

Existing mechanisms and protocols to ensure the integrity of subsector communications provide an initial basis to meet these challenges. Other government agencies have also developed authentication protocols that could be adapted for use in grid security emergencies. For example, the *DoD Cybersecurity Discipline Implementation Plan* (February 2016) offers detailed guidance to strengthen authentication in the face of adversary

efforts to exploit communications networks and devices.<sup>208</sup>

Adversaries may also seek to gain access to classified or operationally sensitive emergency orders. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as possible, lest those operations create incentives for adversaries to strike before their advanced persistent threats were disabled. When attacks are under way, it could be useful to deny adversaries the knowledge of where and how BPS entities are prioritizing the flow of power to vital military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important, given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The FPA and subsequent grid security emergency rule provide for the sharing of classified information in grid security emergencies. The rule specifies that:

To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.<sup>209</sup>

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program already have mechanisms and protocols for sharing and securing classified threat

<sup>206</sup> “About NSTAC,” DHS.

<sup>207</sup> NIAC, *Securing Cyber Assets*, 7.

<sup>208</sup> DOD, *DoD Cybersecurity Discipline Implementation Plan*.

<sup>209</sup> DOE, “RIN 1901–AB40,” 1182.

data with BPS entities cleared for access to that data.<sup>210</sup> Industry and government partners should consider building on those mechanisms to support the issuance of classified emergency orders. Ongoing progress under the Cybersecurity Risk Information Sharing Program will be valuable as it serves a growing array of utilities, accesses additional sources of data and advanced analytic tools, and continues other improvements.

DOE and its partners in industry and government might consider sharing this classified data in other ways. For example, DHS and other federal partners such as the FBI and the National Guard have secure video teleconference capabilities. However, these are technologically complex and not seamlessly interoperable with industry systems. Moreover, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Section 215A addresses this issue by ordering the secretary to “facilitate and, to the extent practicable, expedite,” the security clearance process for key personnel of any entity subject to emergency orders to enable “optimum communication” of threat information.<sup>211</sup> DOE should accelerate its ongoing efforts to meet this requirement. The section also grants the secretary and other appropriate federal agencies the authority to provide temporary access to classified information regarding grid security emergencies and subsequent orders to key personnel of complying entities.<sup>212</sup>

Yet, even for utilities with cleared personnel on their staffs, an even smaller number possess the sensitive compartmented information facilities or other infrastructure and government approvals to store classified information. To address those limitations, the grid security emergency rule clarifies that the secretary may declassify information critical to the

emergency response.<sup>213</sup> But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of combatant commander operational plans; when emergency orders may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

### Communicating with the American People

Adversaries may attack the grid not only to disrupt national defense and the economy but also to gain political leverage over US leaders by inciting public panic and disorder. A presidential declaration that the grid faces imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the US public.

Preplanning for public messaging to accompany grid security emergency declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Unifying messaging with governors and other elected officials on estimated restoration times already presents significant challenges in such events. However, those difficulties will be dwarfed by the problems that adversaries can create through cyber attacks. Attackers may:

- Use information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety
- Intensify state and local requests for defense support to civil authorities to deal with these

<sup>210</sup> “Energy Sector Cybersecurity Preparedness,” DOE.

<sup>211</sup> 16 U.S.C. § 824o–1, (e).

<sup>212</sup> 16 U.S.C. § 824o–1, (b)(7).

<sup>213</sup> DOE, “RIN 1901–AB40,” 1778.

anticipated effects, and thereby put pressure on US leaders to divert scarce defense assets and resources from other missions

- Disrupt normal means of communication on which the public will rely for information about the event
- Magnify the inherent difficulties of estimating restoration times by employing advanced persistent threats that enable repeated reattacks and disruptions in grid service until eradicated from BPS networks.

DHS's Social Media Working Group for Emergency Services and Disaster Management has offered preliminary recommendations on how to counter disinformation during disaster response operations.<sup>214</sup> In addition, the ESCC and its members are developing playbooks to help meet disinformation challenges and support public messaging in the event of cyber or physical attacks against the grid.<sup>215</sup> Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that presidential grid security emergency declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Preplanning for message coordination with Canada and Mexico could also be helpful and might leverage the FPA's provisions for such multinational consultations concerning the issuance of emergency orders.<sup>216</sup>

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. For example, some orders that will be valuable for protecting grid reliability, including those for prioritized load shedding, could

cut off electricity to many thousands of customers to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

## The Deeper Value Proposition for Emergency Orders: Political Top Cover, Waivers, and Cost Recovery

The grid security emergency provisions of the FPA do not even mention a significant advantage that orders can provide for industry: they can help protect power companies from the political heat that extraordinary grid protection measures will create. The FPA's provisions for regulatory waivers and cost recovery offer more explicit benefits. Yet, given the risks that utilities could incur in conducting emergency operations, and the investments in infrastructure that may be required to facilitate order implementation, Congress and DOE should consider additional measures to help power companies defend the grid and protect national security.

### Facilitating Operations under Extraordinary Political Circumstances

In responding to natural hazards, power companies can fall under intense pressure to serve the priorities of state and local elected officials. In severe weather events, for example, governors have told utilities to delay sending restoration resources to assist neighboring states until service has been restored to *all* customers (i.e., voters) in the governors' own states.

Cyber and physical attacks on the grid could create still more intense political pressure, and complicate utilities' efforts to serve national priorities versus those most urgent to meet state and local needs. Such attacks will occur in the context of broader risks of all-out war and will magnify public fears in ways that hurricanes or other natural hazards cannot—especially if those attacks are accompanied by

<sup>214</sup> Social Media Working Group for Emergency Services and Disaster Management, *Countering False Information*.

<sup>215</sup> ESCC, "ESCC: Electricity Subsector Coordinating Council."

<sup>216</sup> 16 U.S.C. § 824o-1, (b)(3).

information warfare operations to incite public panic. Governors will have powerful incentives to ensure that utilities in their states take care of their own citizens rather than meeting requests for assistance from power companies in other states.

However, from a national security perspective, not all states and customers within them will be of equal importance for protecting defense critical electric infrastructure. Some low-population states served by utilities with only limited resources are the homes of vital military installations. These utilities may need assistance from out-of-state power companies to supplement their own personnel and response capabilities when adversaries strike.

The electric industry's Cyber Mutual Assistance (CMA) Program will be critical for providing such support.<sup>217</sup> DOE is expanding the technical resources and capabilities available to support CMA response operations.<sup>218</sup> Under the national response event initiative, investor-owned utilities (led by the Edison Electric Institute) are also bolstering mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States.<sup>219</sup> All of these initiatives will be vital for responding to grid security emergencies that entail multiregional disruptions of the BPS or degrade critical electric infrastructure that the infrastructure's owners cannot restore on their own.

Yet, the voluntary nature of these mutual assistance systems could present challenges in grid security emergencies. In hurricanes or other natural hazards, governors and utilities can predict whether or not their states are likely to be struck and either husband their resources accordingly or provide them in response to requests for assistance. Cyber and physical attacks by Russia, China, or other potential adversaries are much less predictable. Enemies may

strike one region before moving on to others. Attacks could even occur on a nationwide basis. Accordingly, elected officials may discourage utility leaders from volunteering resources for mutual assistance in neighboring regions, even if their own states have not yet been struck.

Issuing emergency orders can help utilities address these challenges and serve national priorities. Participants in the Cyber Mutual Assistance Program are already taking steps to account for the risk of multiregional attacks. DOE and its industry partners should preplan to reinforce those measures in grid security emergencies. If the secretary orders utilities to help protect or restore grid reliability beyond their service areas, those orders will help justify (and indeed, legally require) providing such assistance, regardless of the political pressure against doing so. DOE should consider reaching out to state and local leaders and their senior energy appointees before emergencies occur in order to ensure that they are familiar with the FPA requirements and the national security value of mutual assistance.

Emergency orders can also help utilities execute politically unpopular emergency operational decisions within their own service areas. Cyber and physical attacks could put utility CEOs in the unenviable position of having to manage shortfalls in available power by depriving lower-priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The secretary of energy can give CEOs political top cover for taking such unpopular actions, rather than leave them to act on a voluntary basis and bear the full brunt of explaining why they did so.

Exercises can help utilities and government officials prepare to collaborate in the face of intense political pressures, and coordinate the execution of emergency orders on a nationwide basis. NERC already requires BPS entities to exercise their individual emergency and power system restoration plans. In the GridEx exercise series, over one hundred utilities across the

<sup>217</sup> ESCC, "Cyber Mutual Assistance Program."

<sup>218</sup> DOE, *Multiyear Plan*, 29.

<sup>219</sup> EEI, *Understanding the Electric Power Industry's Response and Restoration Process*.



United States and Canada test the use of their plans against combined cyber-physical attacks and exercise the use of Cyber Mutual Assistance protocols and procedures. Building template emergency orders and utility-specific implementation plans will provide an even stronger basis for coordinated multientity exercises. In planning for GridEx V in 2019, NERC and its government and industry partners should consider the possibility of exercising the issuance and implementation of specific template emergency orders. State, local, tribal, and territorial participation in utility exercises that include the use of emergency orders will also be crucial.

### Environmental, Regulatory, and Legal Waivers

In amending the FPA to address grid security emergencies, Congress provided power companies with an important protection for complying with emergency orders—one that they might not receive by implementing equivalent emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate FERC-approved grid reliability standards or other rules or provisions under the FPA, the act specifies that those actions “shall not be considered a violation” of those provisions. Such waivers of enforcement apply unless a complying entity acts in a “grossly negligent manner.”<sup>220</sup>

The FAST Act amendments to the FPA also introduced broader protections into section 202(c), absolving entities from violations of federal, state, or local environmental laws or regulations that occur as a result of complying with an order. That provision shields complying entities from “any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation.”<sup>221</sup> These protections apply to section 215A emergency orders as well.<sup>222</sup>

FPA-based waivers will be especially valuable for certain types of emergency orders. For example, if the secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service, such as proactively shedding firm load, could also violate NERC’s FERC-approved reliability standards.<sup>223</sup> Separating preplanned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards as well.

The waiver process under the FPA is structured to function automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that a BPS entity has acted with gross negligence. Nevertheless, industry, DOE, and regulators might find it useful to build consensus on the types of waivers that specific template orders should include.

Their discussions could also help address more far-reaching regulatory issues that grid security emergencies may pose. For example, the FPA does not provide waivers for Nuclear Regulatory Commission regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the commission would enforce a violation of its regulations by a nuclear generation entity complying with an emergency order. The worst time to adjudicate such a dispute, however, would be in the midst of a grid security emergency. Pre-event discussions will be particularly important given the nuclear fleet’s imperative to protect public health and safety. DOE, the Nuclear Regulatory Commission, and their industry partners will need to ensure that assessments of regulatory issues associated with

<sup>220</sup> 16 U.S.C. § 824o–1, (f)(4).

<sup>221</sup> 16 U.S.C. § 824a, (c)(3).

<sup>222</sup> 16 U.S.C. § 824o–1, (f)(2).

<sup>223</sup> For example, in events such as the September 2011 Arizona–California disturbance, FERC has found that load shedding led to violations of NERC’s reliability standards.



emergency operations take safety considerations into full account.

Preplanning will also be vital for emergency orders that support power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that “the storage of strategically located spare large power transformers” and other critical grid components “will reduce the vulnerability of the United States to multiple risks facing electric grid reliability,” including cyber and physical attacks.<sup>224</sup> Accordingly, Congress required DOE to develop a strategic transformer reserve plan to determine the number and type of spare large power transformers that should be stored and to examine issues associated with transporting those spares.<sup>225</sup>

DOE responded to this requirement by providing a strategic transformer reserve report (March 2017). The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a more substantial pool of spare large power transformers than DOE had anticipated and that a federally owned reserve is not needed.<sup>226</sup> However, the plan also found that it was crucial to ensure that large power transformers can be efficiently moved during national emergencies.<sup>227</sup>

Regulatory waivers can play a critical role in facilitating that movement. The higher-voltage classes of large power transformers, including 765-kilovolt transformers, are as big as a house and can be moved—slowly and very carefully—only by specialized heavy-haul trucks, railcars, and barges. Under the auspices of the ESCC, utilities have established the Transformer Transportation Working Group to analyze the problems posed by moving large power transformers in an emergency

and to build collaborative plans with transportation companies and associations. A central finding of the group’s analysis: regulatory waivers will be critical to expedite the movement of large power transformers, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.<sup>228</sup>

DOE’s 2017 transformer report committed the department to coordinating with the Transformer Transportation Working Group “to improve and optimize transportation planning in response to a significant national event impacting the electricity grid.”<sup>229</sup> However, the report did not examine how emergency orders and implementation plans might speed the transportation of large power transformers. As DOE collaborates with the working group and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols that are not addressed by the FPA and that pose the greatest impediments to transformer movement. DOE and its partners should then preplan to waive these provisions if the secretary issues emergency orders.

The challenge for such preplanning: the secretary of energy lacks the statutory authority to waive key transportation regulations. Most federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of DOT. Federal regulations and emergency operations that would govern the movement of transformers on barges, which could be critical for restoring power for coastal cities and along the Mississippi–Ohio river system of inland waterways, are overseen by the US Coast Guard and the US Army Corps of Engineers. State and local transportation regulations and permitting requirements will also

<sup>224</sup> FAST Act, 1779.

<sup>225</sup> FAST Act, 1780–1782.

<sup>226</sup> DOE, *Strategic Transformer Reserve*, 21.

<sup>227</sup> DOE, *Strategic Transformer Reserve*, 1.

<sup>228</sup> ICF, *Assessment of Large Power Transformer Risk Mitigation Strategies*, 22–23.

<sup>229</sup> DOE, *Strategic Transformer Reserve*, 22.

pose major impediments to moving large power transformers over roads unless adequate waivers are in place to lift restrictions.

DOE should build collaborative plans to employ waiver authorities beyond those directly under the secretary's control. For example, to facilitate the movement of large power transformers, gubernatorial disaster declarations could help waive state-level regulations. The American Association of State Highway and Transportation Officials and National Emergency Management Association are exploring the use of these and other waiver authorities. DOE is also preplanning with other federal, state, local, tribal, and territorial agencies to coordinate response operations under Emergency Support Function #12—Energy.<sup>230</sup> Especially valuable, a growing number of individual power companies are creating contingency plans for emergency transportation with government agencies and road, rail, and barge companies. Building on these efforts, and on initiatives led by the Transformer Transportation Working Group,<sup>231</sup> the electricity subsector and its partners should establish systematic, nationwide plans to facilitate the movement of transformers and other critical equipment in grid security emergencies.

Over the longer term, Congress, industry, and government partners should also consider whether complying entities should have liability protections beyond those currently provided by the FPA. Prioritized load shedding for extended periods will create “winners and losers” in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other section 9+ assets may leave shortfalls in electric service at dialysis centers, small urgent-care centers, and facilities for special-needs citizens. These disruptions will put lives at risk. Legislators, DOE, and electric industry leaders should examine whether utilities complying

with such necessary but highly disruptive emergency orders ought to have additional liability protections. Cutting off power to lower-priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.<sup>232</sup> Again, if these risks of exposure are sufficiently severe, Congress should consider providing further protections for BPS entities.

### **Cost Recovery for Emergency Operations and Support for Investments in Grid Infrastructure**

Complying with emergency orders may force utilities to incur costs beyond their normal operating expenses. The FPA states that if FERC determines “that owners, operators, or users of critical electric infrastructure have incurred substantial costs” in complying with an emergency order, FERC shall “establish a mechanism that permits such owners, operators, or users to recover such costs.”<sup>233</sup> Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other orders could require reimbursement through FERC-directed mechanisms as well.

The act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that emergency orders require utilities responsible for defense critical electric infrastructure to take emergency measures, the “owners or operators” of critical defense facilities that rely on such infrastructure “shall bear the full incremental costs of the measures.”<sup>234</sup> Fair warning to DOD: it

<sup>230</sup> “State and Local Energy Assurance Planning.” DOE.

<sup>231</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>232</sup> Frankel, “Can Customers Sue Power Companies for Outages?”

<sup>233</sup> The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs “prudently” and that those costs “cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users.” 16 U.S.C. § 824o–1, (b)(6)(A).

<sup>234</sup> 16 U.S.C. § 824o–1, (b)(6)(B).

should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- attacks create major blackouts and deprive utilities of revenue;
- emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- adversaries disrupt financial markets, either through direct cyber attacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.<sup>235</sup>

Power companies are strengthening their plans and capabilities for cross-sector support with the financial services sector.<sup>236</sup> These efforts should include the development of contingency plans for financial-services companies (in coordination with the Department of Treasury and DOE) to help utilities cover the urgent expenses they may incur in responding to grid security emergencies. In addition, to facilitate the reimbursement process provided for in the FPA, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with orders will be more difficult once attacks are under way.

Cost recovery for investments in grid infrastructure to facilitate emergency order implementation will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. Other orders may be impossible to execute unless BPS entities make additional investments in infrastructure. It will be near useless to order transmission operators to protect or rapidly restore service to vital but remote military bases served by a single transmission line if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure that these facilities can help defeat US adversaries when the nation is under attack. DOD will need to develop a cost-recovery mechanism to reimburse defense critical electric infrastructure owners for making such investments.

To be even remotely viable as an emergency order design option, most preplanned power islands will also require at least some infrastructure construction. Ideally, these preplanned islands will use existing generation, transmission, and distribution assets within their service footprints to separate from the grid and still be able to provide reliable electric service to the section 9+ assets inside their borders. But many areas that might be designed to function as islands in a grid security emergency will lack adequate infrastructure to do so. The grid's interconnected design enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Preplanned power islands will not only lose those reliability benefits, but they will also have to make do with infrastructure that utilities built and aligned to be supporting components of the interconnected grid—not self-sustaining islands that would be stood up in grid security emergencies. Moreover, operating and recovering from preplanned island schemes will create an entirely different operating mode than industry is currently designed

<sup>235</sup> NERC, *GridEx III Report*, 15.

<sup>236</sup> See, for example, the Strategic Infrastructure Coordinating Council (SICC). ESICC, "ESICC: Electricity Subsector Coordinating Council."

for. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: to be effectively implemented, many emergency orders could require spending on new transmission lines and other grid infrastructure.

The FPA provisions for grid security emergencies do not explicitly authorize reimbursement for infrastructure investments. While the act requires FERC to establish a mechanism to enable owners, users, and operators of critical and defense critical electric infrastructure to recover their costs of complying with emergency orders, those funding provisions do not mention preattack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover costs for infrastructure investments in resilience against cyber and physical attacks.<sup>237</sup> FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate emergency order execution.

Similar discussions will be necessary with state public utility commissions. As noted above, local distribution systems will play vital roles in implementing emergency orders. Public utility commissions have primary regulatory authority over such distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. They could also make important contributions to reviewing proposed implementation plans for emergency orders that would be executed within their respective states, particularly when local distribution systems would be necessary to implement the orders.

<sup>237</sup> See, for example, FERC, *Extraordinary Expenditures* (96 FERC ¶ 61,299), 1; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), 10–11; and FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), 60.

The FPA opens the door to such discussions. The act states that FERC and the secretary of energy “shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions.”<sup>238</sup> Initiating these discussions with the National Association of Regulatory Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has extensively analyzed criteria for assessing the prudence of investments against cyber and physical attacks and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

## Conclusions and Recommendations for Broader Progress

Taken together, the options for industry–government collaboration examined in this report constitute a massive undertaking for which Congress appropriated zero funding to utilities. Developing a sequenced, prioritized strategy to explore these options will help make doing so a more manageable task.

Potential emergency orders will differ not only in terms of the phases of an attack in which they would be most useful, and in the degree to which they will disrupt normal electric service, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create—especially those that fall into the no-regrets category. Utilities frequently use conservative operations to help protect grid reliability in severe weather events. A growing number of companies are

<sup>238</sup> 16 U.S.C. § 824o–1, (d)(4).



already building on that foundation to draft equivalent conservative operations against cyber and physical threats. Emergency orders based on these initiatives constitute “low-hanging fruit”; creating such orders offers an immediate opportunity for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging emergency order initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are under way, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. Improving communications survivability and preplanning to counter disinformation campaigns will also be crucial for grid security emergency preparedness. So, too, will be efforts not only to fully leverage the FPA’s regulatory waiver and cost recovery mechanisms but also to explore additional liability protections and other measures to help entities comply with emergency orders.

A comprehensive plan to align and integrate these initiatives should also address three additional opportunities to build resilience for grid security emergencies: (1) preplanning to use additional federal and state emergency authorities to defend natural gas systems, communications networks, and other infrastructure on which the grid depends; (2) coordinating with Canada, Mexico, and other nations whose grids may be struck in conjunction with attacks on US electric systems; and (3) exploring new options to deter and defeat attacks on the grid by integrating defensive measures with government operations to blunt further strikes on US power companies and other targets.

## Employing Additional Emergency Authorities for Cross-Sector Resilience

Building preparedness against attacks on the grid is necessary but not sufficient to protect BPS reliability. In many US regions, power generation is becoming extraordinarily dependent on the flow of natural gas. Adversaries may attempt to cause cascading blackouts and other major grid instabilities by crippling natural gas systems. To hedge against such disruptions, some generators have the ability to operate on diesel and other secondary fuels if attackers interrupt gas supplies. But the refining and transportation systems needed to resupply such “dual-fuel” generators with diesel will themselves be at risk in grid security emergencies.<sup>239</sup> Moreover, as examined earlier in this report, coordinated grid restoration will also depend on the availability of communications systems and other infrastructure sectors.

This report has focused on employing the emergency authorities that Congress incorporated into the FPA by creating section 215A of the act in 2015. However, these authorities apply only to BPS owners and operators. The secretary cannot issue emergency orders under 215A to operators of natural gas and diesel fuel systems, much less to telecommunications companies and other infrastructure owners beyond the energy sector. The secretary has a range of other emergency authorities, including the Defense Production Act (DPA) and the authorities provided by section 202(c) of the FPA, which could facilitate coordinated response and restoration operations across the energy sector. The analysis that follows examines how DOE and its industry partners could preplan for the integrated use of all such authorities in a grid security emergency. This analysis also examines how federal and state leaders might use additional emergency powers to coordinate multisector response operations.

---

<sup>239</sup> The author has advised Exelon Corporation on risks of fuel interruptions for power generation. Exelon has provided no funding for this report.



## Coordinating Emergency Operations among Electric Utilities, Natural Gas Systems, and Other Energy Sector Components

Natural gas is an increasingly important source of fuel for power generation in many regions of the United States. Between 2002 and 2016, the nationwide share of electricity provided by gas-fired units increased from 18 percent to approximately 34 percent.<sup>240</sup> However, in New England, California, and other parts of the United States, natural gas has become the predominant source of fuel for power generation.

ISO New England has highlighted the risks that this reliance creates for grid resilience. It notes that “in New England, the most significant resilience challenge is fuel security—or the assurance that power plants will have or be able to obtain the fuel they need to run, particularly in winter—especially against the backdrop of coal, oil, and nuclear unit retirements, constrained fuel infrastructure, and the difficulty in permitting and operating dual-fuel generating capability.”<sup>241</sup>

Other regions also face growing fuel supply risks to grid resilience. A DOE-sponsored report titled *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units, Volume I: The Critical Role of Thermal Units During Extreme Weather Events* (March 2018) notes that many regional transmission organizations and independent system operators will face a combined challenge of inadequate natural gas pipeline infrastructure and competing demands for fuel from users apart from power generators.<sup>242</sup> More broadly, NERC has found that “the electric sector’s growing reliance on natural gas raises concerns regarding the ability to maintain BPS reliability when facing constraints on the natural

gas delivery systems.”<sup>243</sup> NERC’s 2016 *Long-Term Reliability Assessment* also notes that “as part of future transmission and resource planning studies, planning entities will need to more fully understand how impacts to the natural gas transportation system can impact electric reliability.”<sup>244</sup> Additionally, in *Grid Resilience in RTOs and ISOs* (January 2018), FERC called for additional data to better assess the risks posed by “wide-scale disruption to fuel supply” that could result in outages of multiple generators.<sup>245</sup>

Companies in the oil and natural gas subsector are bolstering their capabilities to protect their critical system components from attack and are taking new measures to ensure the continued safe and reliable delivery of natural gas to critical customers, including power generators.<sup>246</sup> However, threats to the oil and natural gas subsector are rapidly escalating as well.<sup>247</sup> As gas system owners and operators address these increasing threats, new opportunities will emerge for joint gas–electric resilience initiatives and emergency planning.

The oil and natural gas and electricity subsectors are already improving their coordination on resilience issues.<sup>248</sup> Moreover, NERC has been facilitating coordination between BPS entities and natural gas companies to address fuel resilience and interdependency challenges.<sup>249</sup> The ESCC has also been developing new coordination mechanisms for the

<sup>240</sup> DOE, *Staff Report to Secretary*, 90.

<sup>241</sup> ISO-NE, “Response of ISO New England Inc.,” 1.

<sup>242</sup> NETL, *Reliability, Resilience and the Oncoming Wave*, 4, 14, 22, 3.

<sup>243</sup> NERC, *Short-Term Special Assessment*, 12. See also NERC, *2013 Special Reliability Assessment*.

<sup>244</sup> NERC, *2016 Long-Term Reliability Assessment*, 21.

<sup>245</sup> FERC, *Grid Resilience*, 161 FERC ¶ 61,012 (2018), 14. See also Stockton, *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*.

<sup>246</sup> “Cybersecurity,” American Gas Association.

<sup>247</sup> Sobczak, Northey, and Behr, “Cyber Raises Threat”; and Stockton (on behalf of Exelon Corporation), *Prepared Direct Testimony* (Docket No. RM18-1-000), 13.

<sup>248</sup> DOE, *Staff Report to Secretary*, 94; and EIS Council, *E-PRO Handbook II*, 189.

<sup>249</sup> NERC, *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*, 1.

two industries (as well as with communications and financial services sectors).<sup>250</sup> Additionally, the natural gas industry participated in GridEx IV, which examined opportunities to mitigate the risk that adversaries will simultaneously attack gas and electric systems.

Building on these and other collaborative efforts, gas and electric companies (and their regulatory partners) should examine how they can prioritize support for each other in grid security emergencies. For example, when blackouts occur, electric companies typically prioritize the restoration of service to compression stations and other electricity-dependent gas infrastructure that is essential to supply fuel for power generation and other critical customers. Support for gas infrastructure should remain a priority, even as BPS entities add other section 9+ facilities to their restoration plans. Gas companies might also reassess their curtailment policies to help gas-dependent BPS entities sustain service to major military installations and other vital facilities in grid security emergencies.<sup>251</sup>

BPS entities and DOE should also pursue deeper collaboration with the companies that refine and deliver secondary fuels for power generation. If adversaries interrupt the flow of natural gas, dual-fuel generators can use diesel, no. 2 fuel oil, or other secondary fuels to sustain their operations in a grid security emergency.<sup>252</sup> However, cascading blackouts could disrupt the flow of these secondary fuels as well. Refining and transportation systems components that are essential to resupply dual-fuel generators depend on electricity. Adversaries may also attack these systems at the same time they strike the grid. Moreover, ongoing cutbacks in industry delivery capacity could magnify these risks of interruption. ISO New England notes that a “withering

delivery supply chain” constitutes an “unquantifiable X factor” in assessing grid resilience.<sup>253</sup> Preplanning to prioritize the delivery of secondary fuels for power generation will be essential for grid security emergencies, especially given the enormous demand for diesel from emergency power generators from hospitals, water utilities, and other vital facilities in wide-area blackouts.

Emergency authorities beyond 215A can help prioritize the flow of natural gas and secondary fuels to protect and restore grid reliability. The DPA will be especially helpful in this regard. The act is the “primary source of presidential authority to expedite and expand the supply of critical resources from the U.S. industrial base to support the national defense and homeland security.”<sup>254</sup> The DPA defines national defense to include “critical infrastructure protection and restoration,” encompassing all electric system components and supporting fuel supply infrastructure (including natural gas pipelines) that are at risk of cyber and physical attacks.<sup>255</sup> In 2012, the White House delegated many of the president’s DPA authorities to the heads of relevant federal agencies, including the secretary of energy for prioritization and allocation decisions regarding “all forms of energy.”<sup>256</sup>

Especially valuable for cross-sector resilience, DOE has established an Energy Priorities and Allocations System that enables the department to prioritize contracts for the delivery of natural gas, diesel, and other energy resources between the companies that provide them and government agencies, electric utilities, and other private and public sector customers. The system also enables DOE to allocate energy materials, services, and facilities to promote

<sup>250</sup> ESCC, “ESCC: Electricity Subsector Coordinating Council.”

<sup>251</sup> EIS Council, *E-PRO Handbook II*, 219.

<sup>252</sup> ISO-NE, *Operational Fuel-Security Analysis*, 52; and NERC, *2013 Special Reliability Assessment*, 4.

<sup>253</sup> ISO-NE, *Operational Fuel-Security Analysis*, 14, 16.

<sup>254</sup> DHS, *Power Outage Incident Annex*, 129.

<sup>255</sup> 50 U.S.C. § 4552, (14).

<sup>256</sup> Obama, *Executive Order—National Defense Resources Preparedness*.

“critical infrastructure protection and restoration” and emergency preparedness.<sup>257</sup>

DOE has already used its authorities under the DPA to support power generation in previous energy crises. In 2001, for example, the department used these authorities to ensure that emergency supplies of natural gas continued to flow to Californian power generators, thereby helping to avoid threatened electrical blackouts.<sup>258</sup> Now, to build preparedness for grid security emergencies, DOE and its industry partners should consider preplanning to use the DPA to sustain or restore gas and diesel deliveries to critical generators, including those that serve microgrids on defense installations, regional hospitals, and other assets critical for national security and public health and safety.

DOE could use the DPA to support and prioritize power restoration operations in other ways as well. Section 101(a) of the act provides DOE with the authority to prioritize the delivery of critical grid components in an emergency. If coordinated physical attacks damage or destroy transformers at a large number of critical substations, the secretary could use the DPA to allocate replacement transformers in ways that most directly benefit national security and public health and safety.

Two additional sources of emergency authorities could further strengthen preparedness and supplement the use of section 215A emergency orders. The first is section 202(c) of the FPA. The section authorizes the secretary to order “temporary connections of facilities and such generation, delivery, interchange, or transmission of electric energy as in its judgment will best meet the emergency and serve the public interest.” That provision also specifies that the secretary could exercise such powers “during the continuance of any war in which the United States is engaged, or whenever the Commission determines that an

emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy or of facilities for the generation or transmission of electric energy, or of fuel or water for generating facilities, or other causes.”<sup>259</sup>

A key virtue of section 202(c) is that the secretary can apply these emergency authorities to local distribution systems that might not fall within the purview of section 215A. Moreover, DOE has a strong record of having used 202(c) authorities in past emergencies, including the California Enron crisis, Hurricane Katrina, and other events.<sup>260</sup> DOE and its industry partners should consider building on this foundation to plan for the use of these authorities in grid security emergencies.

The Natural Gas Policy Act provides further authorities that could help coordinate energy sector operations in grid security emergencies. The president must declare a natural gas supply emergency before the secretary gains emergency powers under the act. The president can make such a declaration if there is evidence of an imminent or existing “severe natural gas shortage, endangering the supply of natural gas for high-priority uses” and that, having exhausted other alternatives “to the maximum extent practicable,” natural gas emergency authorities are necessary to resolve the situation.<sup>261</sup> The president may also delegate this authority, as well as the authority to issue rules or orders, to the secretary of energy or other appropriate federal officials.<sup>262</sup>

The president or secretary can issue two main types of orders or rules. Most important, during a natural gas supply emergency, the act authorizes the president or other officials to allocate natural gas supplies “to assist in meeting natural gas requirements for high-priority

<sup>257</sup> DOE, “RIN 1901-AB28,” 33615, 33622-33626.

<sup>258</sup> Brown and Else, *Defense Production Act of 1950*, 10.

<sup>259</sup> 16 U.S.C. § 824a, (c)(1).

<sup>260</sup> “DOE’s Use of Federal Power Act Emergency Authority,” DOE.

<sup>261</sup> 15 U.S.C. § 3361, (a).

<sup>262</sup> 15 U.S.C. § 3364, (d).

uses.”<sup>263</sup> The secretary could use this provision to ensure that critical generating facilities get the fuel they need.

Of course, some of these authorities overlap. DOE and its government and industry partners should develop an integrated approach to employing these powers for grid security emergencies, and determine which particular authorities are best suited to meet specific energy sector risks that cyber and physical attacks can create. These partners, along with other energy sector stakeholders, should also consider exercise scenarios that involve the simultaneous use of multiple emergency authorities to simulate the complex legal environment they may be faced with in a grid security emergency.

### **Multisector Resilience for Grid Security Emergencies**

An overarching strategy for grid security emergency preparedness should also advance operational coordination between energy companies and other infrastructure sectors that both rely on electricity and play vital roles in power restoration. Additional federal emergency authorities and incident response plans can help strengthen coordination between these interdependent sectors.

Using this broader array of plans and authorities will be particularly important if adversaries simultaneously attack multiple infrastructure sectors. By striking other sectors together with the grid, adversaries can exploit interdependencies between them to maximize the attack’s disruptive effects on national security, including the ability of defense installations and supporting civilian infrastructure to conduct operations abroad.<sup>264</sup> The *National Cyber Incident Response Plan* provides a framework for strengthening multisector coordination mechanisms for such attacks. As the administration refines the

plan, DOE and its government and industry partners should ensure that the issuance and execution of emergency orders fit within this broader framework and directly contribute to multisector resilience.

Updates to the *National Response Framework* and other FEMA-led initiatives can offer further benefits for grid security emergencies. In its after-action report from the 2017 hurricane season, FEMA noted that emergency managers and their private sector partners lack the multisector coordination mechanisms necessary to accelerate the restoration of electric power and other lifeline services.<sup>265</sup> The report called for FEMA to build “a cross-sector approach to the Agency’s planning, organizing, response, and recovery operations,” and revise current national-level planning frameworks to create a cross-sector emergency support function.<sup>266</sup> DOE and industry should partner to prioritize support for power sustainment and restoration within this broader initiative.

The *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans* provides a prime opportunity to embed cross-sector coordination efforts in regional incident response plans.<sup>267</sup> The annex calls for the development of regional plans to build resilience against extended multistate blackouts and ensure that interdependent sectors can accelerate power restoration while also countering threats to public health and safety.<sup>268</sup> In many areas of the United States, utilities are already helping DOE, FEMA, and their state and local partners build such plans for their regions. Cross-sector preparedness for grid security emergencies should become a key focus of future power outage incident planning efforts.

<sup>263</sup> 15 U.S.C. § 3363, (a).

<sup>264</sup> Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee*, 11.

<sup>265</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 13.

<sup>266</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 12–13.

<sup>267</sup> EIS Council, *E-PRO Handbook III*, 45.

<sup>268</sup> DHS, *Power Outage Incident Annex*, 77.



In all of these planning and operational coordination initiatives, DOE and other departments responsible for specific infrastructure sectors should examine how other federal emergency authorities might supplement those that apply to the energy sector. The communications sector provides one such opportunity. The president has extensive authorities to address national security and emergency preparedness telecommunications issues under the Communications Act, including the power to prioritize the use of communications capabilities and provide complying entities with legal and regulatory protections.<sup>269</sup> Executive Order 13618 assigns many of these authorities and associated responsibilities to federal departments and agencies. The secretary of commerce, for example, is responsible for developing plans and procedures for emergency use of radio frequencies and other communications systems.<sup>270</sup> The secretary of homeland security is responsible for overseeing the development, testing, and implementation of emergency communications capabilities.<sup>271</sup> Using these capabilities to support power restoration could be enormously helpful in grid security emergencies. Equivalent emergency authorities for other sectors could assist restoration as well. However, as with all such opportunities, effectively using these federal authorities will depend on extensive preplanning.

State governors are likely to invoke their own authorities to respond to grid security emergencies. Governors have primary responsibility for protecting the health and safety of their citizens. Cyber and physical attacks on the grid, especially if paired with strikes against communications systems and other interdependent sectors, could disrupt hospitals, water systems, and other assets on which their citizens rely. Governors in every state have the ability to declare emergencies and issue executive orders to help deal

with such threats to public health.<sup>272</sup> A growing number of states are also including utility representatives in their emergency operations centers, building collaborative plans and coordination mechanisms to respond to attacks on the grid, and preparing for state National Guard personnel to help utilities defend and restore the flow of power. These initiatives are bolstering overall preparedness for grid security emergencies. However, if multiple governors employ their own emergency authorities and implement state-level blackout response plans, it will be enormously difficult to coordinate their efforts with federal actions—including the issuance of DOE emergency orders to utilities in those very same states.

The only way to overcome such difficulties is to exercise the use of all of the authorities that could help protect and restore grid reliability, across multiple sectors and with the participation of both federal and state leaders. GridEx IV offered an important step forward in this regard. Exercise participants from the oil and natural gas subsector, as well as the financial-services and communications sectors, contributed perspectives on how they could help utilities respond to cyber and physical attacks on the grid. Representatives from state governments discussed how governors might act in such an emergency. GridEx V will provide an opportunity to address such coordination challenges in greater detail. GridEx V could also exercise the use of specific template emergency orders, together with communications mechanisms and playbooks developed for grid security emergencies. Additional exercises by BPS entities and their partners at all levels of government will also be vital to prepare for the implementation of such orders.

## Extended Partnership Requirements within the United States and Abroad

Congress implicitly imposed geographic constraints on the secretary's authority to issue emergency orders to protect the reliability of defense critical electric

<sup>269</sup> 47 U.S.C. § 606.

<sup>270</sup> Obama, *Executive Order—Assignment*, section 5.3.

<sup>271</sup> Obama, *Executive Order—Assignment*, section 5.2. See also DHS, “Emergency Communications.”

<sup>272</sup> Orenstein and White, “Emergency Declaration Authorities.”



infrastructure. The FPA limits such infrastructure to that which is located in the forty-eight contiguous states or the District of Columbia.<sup>273</sup> However, Alaska and Hawaii are home to vital grid-dependent military installations and supporting civilian infrastructure, including facilities for US continental ballistic missile defense and command and control of military operations in the Pacific region. Key defense installations also exist in Guam and other US territories. As the electric industry and DOE build preparedness for grid security emergencies, they should consider collaborating with the utilities that serve these states and territories and their government partners (including DOD) to strengthen plans and capabilities for coordinated operations.

Close coordination will also be necessary with Canada. The secretary of energy has no authority to issue emergency orders to power companies in other countries. However, the electric grids of the United States and Canada are deeply interconnected. This integration entails both risks and opportunities in grid security emergencies. Adversary-induced blackouts in one nation may cascade across the border, and extraordinary measures taken to restore US grid reliability could affect Canadian systems. Yet, the connectivity between US and Canadian electric systems can also provide unique opportunities to strengthen the security and emergency preparedness of both nations.

A key foundation for binational cooperation in grid security emergencies is already in place. NERC's reliability standards apply to both US and Canadian utilities, providing shared planning and emergency coordination mechanisms on both sides of the border. US and Canadian power companies and government officials should explore how they might supplement these existing mechanisms for

grid security emergencies. The most immediate opportunity to do so will lie in government-to-government consultations. The FPA requires that, to the extent practicable, the secretary of energy shall consult with Canadian authorities before issuing emergency orders.<sup>274</sup> However, the FPA provides no details on the mechanisms by which consultations will be conducted or on whether and how Canadian officials should be informed when the secretary issues emergency orders to US utilities. The analysis that follows examines opportunities to facilitate binational consultation and operational coordination in grid security emergencies.

The FPA also requires that the secretary consult with the Mexican government before issuing emergency orders. While the US and Mexican grids are much less integrated than those of the US and Canada, discussions on grid security emergency preparedness with Mexican officials could also be valuable. Coordination beyond North America may be useful as well. If a severe regional crisis escalates into attacks on the US power grid, US security partners in those regions may face strikes against their own electric systems. Sharing information on whether an attack is imminent and taking coordinated grid protection measures (including those for conservative operations) will help the United States and its allies meet such challenges.

### **Deepening Integration between US and Canadian Grids: Risks and Potential Benefits for Grid Security Emergency Resilience**

DOE notes that "the United States and Canada serve as a global model of highly functional, cross-border electricity coordination."<sup>275</sup> US and Canadian grids are connected by over three dozen major transmission lines, ranging from the Pacific Northwest to New England. The resulting power flows have created a deeply integrated network of north-south BPS infrastructure and synchronized

<sup>273</sup> 16 U.S.C. § 824o-1, (a)(4). The FPA's section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).

<sup>274</sup> 16 U.S.C. § 824o-1, (b)(3).

<sup>275</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-5.

cross-border operations.<sup>276</sup> This integration also provides significant economic and energy security benefits for both countries.<sup>277</sup>

Connectivity between US and Canadian grids will grow still closer in the decades to come.<sup>278</sup> New York and Massachusetts are pursuing significant increases in Canadian hydropower to help achieve their clean energy goals. Several new cross-border transmission lines are also under development, though many of them face permitting challenges. The Lake Erie Connector is a one-thousand-megawatt high-voltage, direct current line expected to link Ontario's Independent Electricity System Operator with PJM in 2020.<sup>279</sup> The Champlain Hudson Power Express from Quebec to New York City is expected to go into service in 2021, with still other projects in various phases of development in New England, the Midwest, and the Pacific Northwest.<sup>280</sup>

These and other projects offer significant economic benefits to both nations. However, the connectivity of US and Canadian power grids also creates risks of cross-border failures. The 2003 Northeast blackout that started in Ohio created power outages for millions of customers in Ontario.<sup>281</sup> Interconnections between US and Canadian power systems have increased since that event. US and Canadian officials warn that given this connectivity, "isolated or complex events with cascading effects that take place in either country can have major consequences for both the United States' and Canada's electric grids and adversely affect national security, economic stability, and public health and safety."<sup>282</sup>

Mandatory reliability standards reduce the risks of outages across North America. In the aftermath of the 2003 blackout, NERC began issuing standards applicable to entities on both sides of the border. NERC reliability standards are mandatory and enforceable in the provinces of Ontario, New Brunswick, Alberta, British Columbia, Manitoba, and Nova Scotia. Twelve such reliability standards also went into effect in Quebec in April 2015; the province is now considering adopting additional standards.<sup>283</sup> These shared US-Canada standards help power companies in both countries maintain the reliability of their systems and will help them prevent instabilities from spreading during grid security emergencies.

NERC's role as the electric reliability organization for North America provides an additional bulwark for binational grid resilience. As Figure 7 illustrates, three NERC regional entities include power companies on both sides of the border: the Northeast Power Coordinating Council (NPCC), the Midwest Reliability Organization (MRO), and the Western Electricity Coordinating Council (WECC). These entities help monitor and enforce compliance with reliability standards and reinforce NERC's integrated approach to reducing the risks of cascading failures and other instabilities.<sup>284</sup> The E-ISAC also provides additional support for utility preparedness in both nations.

However, Russia and other potential adversaries' increasingly sophisticated cyber capabilities pose challenges for protecting power flows between Canada and the United States, just as they do for electric service within each country individually.

Connectivity between US and Canadian power systems offers other benefits for protecting reliability against cyber and physical attacks. For example, as

<sup>276</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-6.

<sup>277</sup> Stanley, *Mapping the U.S.-Canada Energy Relationship*, 9.

<sup>278</sup> Parfomak et al., *Cross-Border Energy Trade*, 34.

<sup>279</sup> "Work Continues on ITC Lake Erie Project," *Transmission Hub*.

<sup>280</sup> Vine, *Interconnected: Canadian and U.S. Electricity*, 9.

<sup>281</sup> NERC Steering Group, *Technical Analysis of Blackout*, 1.

<sup>282</sup> Governments of US and Canada, *Joint United States-Canada Electric Grid Security and Resilience Strategy*, 10.

<sup>283</sup> "North America," NERC. See also "Compliance - Québec," Northeast Power Coordinating Council; and "Electric Power Transmission Reliability Standards," Régie de l'énergie Québec.

<sup>284</sup> "Key Players," NERC.

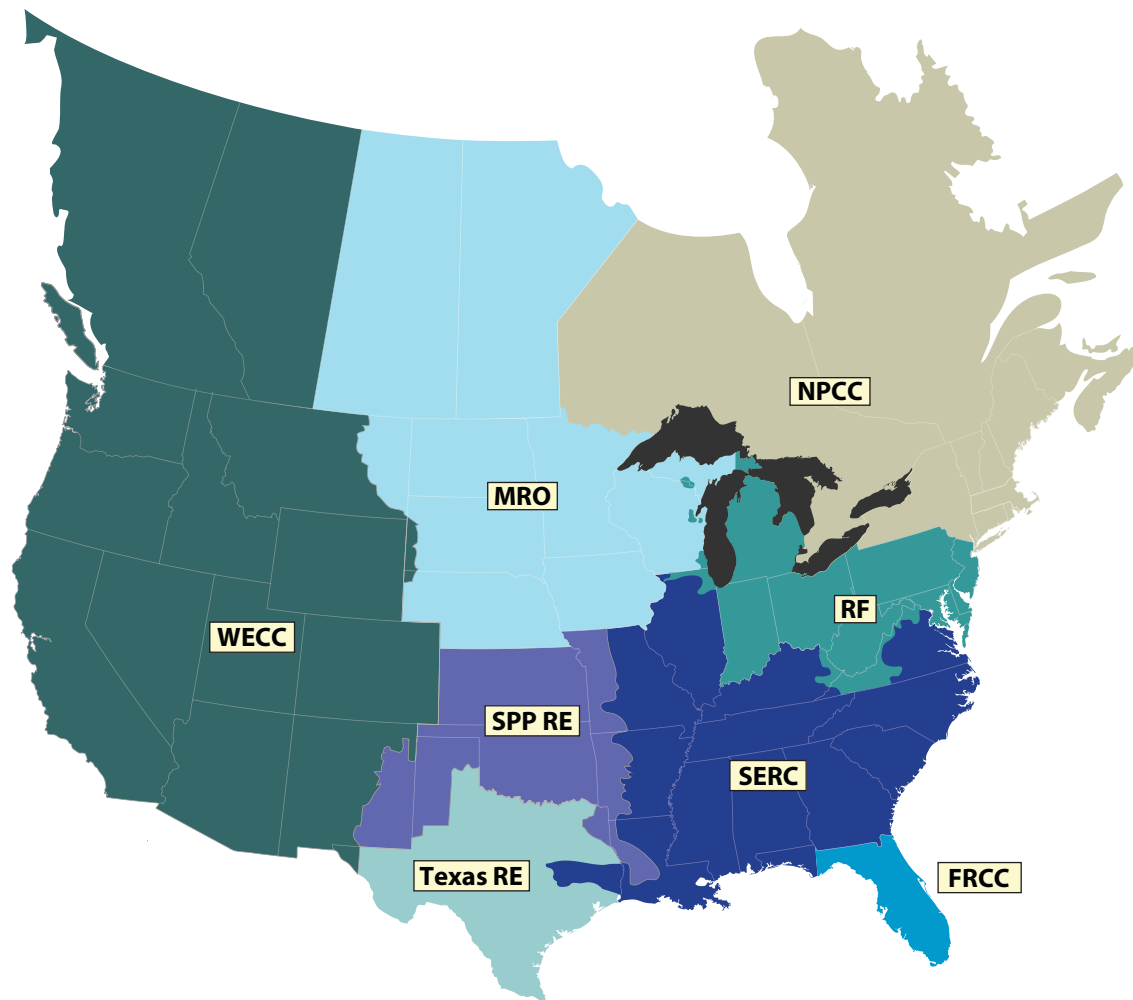


Figure 7. NERC Regional Entities across North America

new transmission lines increase this connectivity, electricity exported by Canada could become increasingly valuable when managing power imbalances in the United States and could make up for sudden shortfalls in the availability of US-generated power. However, we must assume that adversaries know this as well. To maximize the disruption to the US grid and the critical facilities that depend on it, attackers may strike the cross-border transmission lines that would otherwise help US grid owners and operators prevent cascading failures, uncontrolled separations, and other major reliability issues.

Adversaries may also attack grid assets that supply power to critical Canadian defense installations. The United States and Canada have a unique binational

defense system to protect their territories. The North American Aerospace Defense Command plays a vital role for both nations for aerospace warning, aerospace control, and maritime warning for North America.<sup>285</sup> The Canada-US Civil Assistance Plan also helps enable military members from one nation assist the other's armed forces in support of civilian authorities during emergencies.<sup>286</sup> Potential adversaries such as Russia may seek to degrade these binational military capabilities and operations by attacking defense critical electric infrastructure on

<sup>285</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

<sup>286</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

both sides of the border. US and Canadian officials and power companies should plan accordingly for mutual support in grid security emergencies.

### Specific Options for US–Canada Coordination

In addition to requiring US–Canada consultations before the secretary issues emergency orders, the FPA also states that FERC and the secretary “shall, in consultation with Canadian and Mexican authorities, develop protocols for the voluntary sharing of critical electric infrastructure information with Canadian and Mexican authorities and owners, operators and users of the bulk-power system outside the United States.”<sup>287</sup> Those initiatives provide a valuable starting point to build shared North American preparedness for grid security emergencies. However, much deeper collaboration is both possible and necessary, especially with Canada. Options for further analysis are described below.

**Consultative mechanisms, collaborative planning, and coordinated emergency operations.** The FPA does not specify how US officials would consult with their Canadian counterparts if the president declares a grid security emergency. Nor does it discuss whether the president would do so prior to making such a declaration. Exchanges between the US president and the prime minister of Canada would constitute the highest level of binational coordination. More detailed discussions about options for responding to incidents could also occur between the secretary of energy and the Canadian minister of national resources. That minister has the federal lead for electricity issues in Canada but lacks emergency authorities equivalent to those that the FPA grants to the secretary of energy.<sup>288</sup>

However, government coordination mechanisms will also need to include a broader array of participants. Global Affairs Canada and the US State Department might well be involved in any coordination of

binational grid emergency actions, just as they are in other emergency assistance mechanisms.<sup>289</sup> Coordination with state and provincial governments could also be helpful. The 1982 amendments to Canada’s Constitution Act (1867) explicitly recognized provinces’ and territories’ constitutional rights to manage electrical energy.<sup>290</sup> In particular, authority over electricity generation and transmission in Canada rests primarily with provincial governments.<sup>291</sup> It will be essential to account for these features of Canadian governance in building US–Canada consultative mechanisms.

The NERC alert system and other emergency coordination systems provide a solid basis for collaboration between US and Canadian utilities in grid security emergencies. However, the FPA does not address the question of how (and how much) information DOE officials should share with Canada on the issuance of emergency orders to US utilities. Given the deep integration of the US and Canadian grids, maximum sharing could help coordinate both countries’ emergency operations before, during, and after attacks. To facilitate such information sharing, DOE, Natural Resources Canada, and other relevant stakeholders can leverage existing US–Canadian mechanisms to protect sensitive information, supplemented as needed to support grid security emergency coordination.

The *Joint US-Canada Electric Grid Security and Resilience Strategy* (December 2016) provides a policy framework for building these coordination and information sharing mechanisms. The US and Canadian governments developed the strategy “to strengthen the security and resilience of the U.S. and Canadian electric grid from all adversarial, technological, and natural hazards and threats.”<sup>292</sup> The strategy calls for collaboration to protect system assets and

<sup>287</sup> 16 U.S.C. § 824o–1, (d)(5).

<sup>288</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>289</sup> “Compendium,” Public Safety Canada.

<sup>290</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>291</sup> “North America,” NERC.

<sup>292</sup> Governments of US and Canada, *US-Canada Electric Grid Security and Resilience Strategy*, 1.



critical functions in both nations so that the North American grid can “withstand and recover rapidly from disruptions.”<sup>293</sup> The strategy also emphasizes the need for collaboration to manage contingencies and enhance response and recovery efforts.<sup>294</sup> All of these features make the strategy a promising basis for creating the detailed collaborative mechanisms that grid security emergencies will require.

### **Protecting defense critical electric infrastructure.**

While the FPA facilitates the development of emergency orders to protect the flow of power to critical US defense installations, US–Canada coordination in grid security emergencies could also help strengthen power resilience for bases on both sides of the border. The Pacific Northwest exemplifies the potential benefits of such collaboration. Washington State hosts a number of vital installations, including Joint Base Kitsap on Puget Sound, which serves as the homeport for aircraft carriers, attack submarines, and other assets that would be needed for operations in the South China Sea and for other regional contingencies. Canadian Forces Base Esquimalt and other key Canadian installations are located less than one hundred miles away on Vancouver Island. Esquimalt is the second-largest military base in Canada and is home to Maritime Forces Pacific and Joint Task Force Pacific headquarters.<sup>295</sup> Coordinating US–Canada emergency plans to protect the flow of power to these installations could benefit the security of both nations.

The US–Canada Permanent Joint Board on Defense provides an ideal venue to explore such coordination options. Established in 1940 to discuss and advise on issues related to continental defense and security, the board has focused increasing attention on binational opportunities to strengthen critical infrastructure resilience. In 2011, the CEO of NERC led a

Permanent Joint Board on Defense discussion of how North American BPS emergency plans and coordination mechanisms could benefit US and Canadian national security. Natural Resources Canada and DOE have also participated in subsequent Permanent Joint Board on Defense meetings, along with the defense departments of both nations and critical infrastructure stakeholders. US and Canadian officials should consider using the board to facilitate industry–government discussions on opportunities to coordinate in grid security emergencies.

### **Coordination with Mexico and Beyond: Multinational Resilience against Grid Security Emergencies**

The US grid has much less connectivity with Mexican electric systems than with the Canadian grid. Southern California and a portion of Mexico’s Baja California have synchronous interconnections. Along the Mexico–Texas border, asynchronous interconnections also exist between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities.<sup>296</sup> In 2017, Mexican and US officials agreed to nonbinding pledges to increase this connectivity in ways that would strengthen reliability on both sides of the border.<sup>297</sup>

The election of Mexican president Andrés Manuel López Obrador in July 2018 may lead to significant changes in that country’s energy policies.<sup>298</sup> Structural challenges will also slow efforts to increase US–Mexico grid integration, including repeated power shortages and major shortfalls in the functionality of the Mexican grid.<sup>299</sup> Nevertheless, it could be useful to expand discussions with industry and the incoming government on protecting grid reliability against cyber and physical threats.

<sup>293</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 12.

<sup>294</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 11.

<sup>295</sup> “Maritime Forces Pacific,” Royal Canadian Navy.

<sup>296</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–4.

<sup>297</sup> “Increasing Electricity Cooperation in North America,” DOE.

<sup>298</sup> Kissane and Medina, “Energy Aftershocks.”

<sup>299</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–13.



Building grid security emergency coordination mechanisms beyond North America would also be helpful. As noted earlier, attacks on the US grid are most likely to occur in the context of an intense, escalating regional crisis in the Baltics, Northeast Asia, or some other area where US allies and critical security interests are at risk. In particular, adversaries may seek to inflict blackouts that could disrupt the deployment of US forces to the crisis zone. But we should also expect that US allies in the region will suffer attacks on their own grids, aimed at disrupting their ability to conduct combined operations with the United States and deliver electricity to US bases on their territories.

NATO's 2018 Locked Shields exercise focused on building alliance-wide preparedness for cyber and physical attacks against energy and communications systems.<sup>300</sup> In future exercises, allies might explore how to jointly determine whether grid attacks are potentially imminent and coordinate on the implementation of conservative operations across NATO member countries. The United States might explore equivalent opportunities for collaboration with Japan, South Korea, Australia, New Zealand, and other security partners. Existing treaty commitments, including those under Article V of NATO's founding treaty, will provide a starting point to meet our shared grid resilience challenges.<sup>301</sup>

### Playing Defense in Cyberwarfare: Doctrine, Integrated Planning, and Benefits for Deterrence

Utility leaders are urging the federal government to do more to assist them in deterring and defeating attacks on the grid. Their calls come at a perfect time. Administration officials have opened the door to new forms of operational collaboration between industry and government, including "collective

defense" during cyber attacks.<sup>302</sup> This report examines an especially significant option to expand their collaboration: coordinating the implementation of emergency orders with DOD operations to halt attacks at their source.

Deeper operational partnerships can also help meet underlying challenges for cyber deterrence. A number of cybersecurity analysts argue that deterrence by denial is impractical in cyberspace because offensive cyber capabilities are so much stronger than cyber defenses, and because cyber warfare will be very different from conventional conflicts. Analysts also warn that the United States lives in a cyber "glass house": given the vulnerability of the power grid and other infrastructure systems, the president cannot credibly threaten to use cyber weapons to defend US allies and interests. Improving preparedness for grid security emergencies can help address these concerns and support ongoing reassessments of US strategies for deterrence.

### Unity of Effort in Defensive Operations at Home and Abroad

Tom Fanning, CEO of Southern Company (one of the largest power companies in the United States), notes that he and other infrastructure owners and operators face a major constraint on their ability to defend their systems: "I can't fight back."<sup>303</sup> In theory, blunting attacks at their source could greatly ease the scale and severity of the threats that utilities will need to counter. In practice, integrating grid security emergency operations with measures to suppress enemy attacks would entail major policy and technical obstacles.

Power companies should not be responsible for striking enemies' offensive cyber infrastructure during grid security emergencies. The US government is the sole actor with the prerogative to engage in techniques such as "hacking back" that

<sup>300</sup> Cowan, "Locked Shields 2018."

<sup>301</sup> "The North Atlantic Treaty," NATO.

<sup>302</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>303</sup> Smith, "U.S. Officials Push New Penalties."

involve operations to disrupt or destroy an attacker's system.<sup>304</sup> Moreover, even if power companies gained legal authority to fight back against adversaries, their technical capacity to do so would be dwarfed by the capabilities possessed by US Cyber Command and other US government organizations.

Efforts to integrate defensive operations at home and abroad should rest on the comparative advantages of industry and government. BPS entities and other components of the electricity subsector are best positioned to defend their systems from within, assisted by DOE and other government partners. Operations abroad to halt attacks on the grid should remain the exclusive purview of government agencies, supported by industry assistance to gather malware samples and facilitate attack attribution. Based on this division of labor, government and industry leaders could explore whether and how to strengthen unity of effort for the full scope of defensive operations within the United States and beyond.

Secretary of homeland security Kirstjen Nielsen has called for the adoption of a "collective defense" posture that might include such expanded partnerships. Under the collective defense model, industry and government would collaborate to act on threat indicators and "respond more quickly and effectively to incidents."<sup>305</sup> The most familiar realm of operational collaboration lies in government support to help utilities detect, characterize, and eradicate malware on their systems. DHS is strengthening the National Cybersecurity and Communications Integration Center's ability to provide such assistance.<sup>306</sup> State National Guard organizations can also support post-cyber attack power restoration within the larger context of the industry's Cyber Mutual Assistance system.<sup>307</sup> However, in a cyber strike against the

United States, DOD will require many of these same guard personnel to protect the department's networks, conduct cyber operations against the attacker, and carry out other federal missions.<sup>308</sup> Power companies and government agencies will need to continue clarifying whether and how specific National Guard assets can help meet utility requests for assistance; existing doctrine and procedures for providing defense support to civil authorities offer a solid basis to advance those discussions.

In contrast, coordinating industry grid protection measures with government operations to suppress attacks would extend collective defense into uncharted territory. The command vision for US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, offers a starting point to examine how engaging against malicious cyber actors might help protect utilities. The document states that the United States must "increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage." To do so, DOD "is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems."<sup>309</sup>

Forward defense operations could respond to and help counter adversary efforts to implant malware on utility networks. Should such operations also help power companies protect their systems if the president declares that an attack is imminent? As senator Mike Rounds frames the question: "If someone is going to shoot an arrow at you, do you shoot the archer before he shoots the arrow?"<sup>310</sup>

US Cyber Command's vision statement does not directly address this possibility. However, each phase of grid security emergencies will likely offer

<sup>304</sup> GWU, *Into the Gray Zone*, 25.

<sup>305</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>306</sup> Marks, "DHS Stands Up New Cyber Risk Center."

<sup>307</sup> Crowe, "National Guard Preparing"; and Puryear, "91st Cyber Brigade Activated."

<sup>308</sup> DOD, *Cyber Strategy*, 4.

<sup>309</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 4–5.

<sup>310</sup> Bordelon, "Rounds Is Ready."

a different mix of risks and rewards for combining domestic and forward defense operations. For example, if the president determines that an attack on the grid is imminent, the secretary might issue orders for conservative operations to bolster grid defenses at the same moment that forward defense operations disrupted enemy cyber infrastructure poised to launch the strike. But assessments that an attack is imminent may turn out to be wrong. No-regrets orders for conservative operations are valuable precisely because using them will entail few consequences if warning indicators turn out to be false. Preattack forward defense operations could start a cyberwar that might not otherwise have occurred.

The United States can avoid such risks by waiting until attacks on the grid are under way before striking the enemy's offensive infrastructure. However, developing the technical capabilities to identify and disrupt the cyber infrastructure being used in an attack could prove challenging. Moreover, it is not clear whether integrating plans for home and away operations would offer significant benefits, as opposed to relying on utilities and government agencies to conduct those two types of operations independently.

US Cyber Command has opened the door to building new types of partnerships with the electricity subsector. The command has called for measures to "deepen and operationalize" collaboration between the private sector, the armed services, and other command partners.<sup>311</sup> As those efforts go forward with the electricity subsector and DOE, exploring options for collective defense (and clarifying the dangers they might present) should be a prime focus for analysis.

### **Maximizing Industry Contributions to Cyber Deterrence by Denial**

The *National Security Strategy* emphasizes that rather than rely on threats of cost imposition alone

to deter enemy attacks, the United States will also strengthen deterrence by denial. This report has examined how grid security emergency orders and implementation plans can raise adversaries' doubts as to whether they can achieve their objectives. But strengthening this form of deterrence will also entail underlying challenges.

Many cybersecurity analysts believe that offensive cyber capabilities are vastly stronger than defenses against them, and that this preeminence creates destabilizing incentives for adversaries to strike first when conflicts loom.<sup>312</sup> Unless measures to strengthen grid resilience can help weaken the dominance of offense over defense in the cyber realm, deterrence by denial will remain difficult to accomplish against highly capable adversaries.

However, today's offensive dominance stems in part from historical factors that are rapidly changing. The interconnected grid evolved decades ago when no cyber threat existed to drive protective measures. Moreover, as utilities began incorporating computer-assisted controls, sensors, and operating technology systems, few of these companies accounted for the risk that cyber threats to their systems would escalate so rapidly. As noted in this report, utilities are advancing a wide array of technical initiatives and fallback operational plans to counter and (ideally) stay ahead of adversaries' capabilities. In addition, regulatory bodies across the nation are increasingly willing to enable companies to recover costs for cyber resilience.

The current preeminence of offense over defense also reflects organizational factors. Rebecca Slayton has found that historically, "the success of offense is largely the result of a poorly managed defense."<sup>313</sup> The skills of the individuals employing cyber weapons and defensive tools, and the effectiveness with which

---

<sup>311</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 8.

---

<sup>312</sup> For a review of this "offense-dominant" literature, and the smaller set of works opposing it, see Slayton, "What Is the Cyber Offense-Defense Balance?," 72.

<sup>313</sup> Slayton, "What Is the Cyber Offense-Defense Balance?," 87.

these practitioners are managed and organized, have an enormous impact on the outcome of cyber engagements. Slayton notes that the importance of organization for cyber defense is implicit in discussions of the need for better public-private partnerships and information sharing. What has been missing, however, are efforts to make such partnerships *operational* and create unity of effort in government-industry defense actions when adversaries strike. That is precisely the gap that DOE and its industry partners can fill by developing grid security emergency orders and advancing all of the other collaborative initiatives necessary to make those orders effective.

Improved partnerships and technical capabilities to protect the grid cannot by themselves make defense preeminent. To further rebalance offense and defense in cyberspace, resilience initiatives will be necessary across all critical infrastructure sectors, as well as a host of other measures to facilitate the command, control, and coordination of public-private defensive operations. But building preparedness for grid security emergencies will be vital for that broader effort. Moreover, establishing defensive primacy is not necessary to facilitate deterrence by denial. As defined by the *National Security Strategy*, deterrence by denial functions by creating doubt in our adversaries that they can achieve their objectives.<sup>314</sup> DOE and its partners should develop grid security emergency orders that (perhaps in conjunction with forward defense operations) can make adversaries less likely to attack, even if defensive dominance remains out of reach.

Strengthening grid resilience can also support the broader reassessment of the US deterrence posture that is now under way. Robert Strayer, the State Department's deputy assistant secretary for cyber and international communications and information policy, notes that the increasing severity of threats to

US infrastructure is forcing "an evolution in the US government's thinking about how to deter malicious cyber actors."<sup>315</sup> In conventional warfare, deterrence by denial functions by making it physically difficult for adversaries to achieve their objectives and by raising enemy forces' costs of taking their targets.<sup>316</sup> Cyberwarfare will not entail the same sorts of attrition of enemy forces that occurs in battles with tanks, fighter aircraft, and other conventional weapons. The Trump and Obama administrations have redefined deterrence by denial to better fit the characteristics of cyberspace. The unique features of cyber conflict will require continued rethinking of how the United States can strengthen deterrence in the years to come. As utilities and government agencies build resilience for grid security emergencies, new opportunities will emerge to influence adversaries' perceived costs and benefits of attack. The United States should continue to refine its deterrence posture to capitalize on these improvements.

### Escaping the "Glass House" Syndrome

The president may need the ability to use cyber weapons against foreign targets to help resolve crises on terms favorable to the United States. The *DOD Cyber Strategy* (April 2015) states that:

There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an

<sup>314</sup> White House, *National Security Strategy*, 13.

<sup>315</sup> Smith, "U.S. Officials Push New Penalties."

<sup>316</sup> For definitions of classic deterrence by denial derived from conventional warfare, see Gerson, "Conventional Deterrence"; and Mitchell, "The Case for Deterrence by Denial." For an analysis of how that definition differs from that used by the Trump administration, see Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy."



ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests.<sup>317</sup>

However, any such operations against an adversary's cyber infrastructure would risk retaliatory strikes against the United States—including, potentially, attacks on the grid. Senator Thom Tillis (R-NC), a member of the Senate Armed Service Committee, emphasizes that the United States is living in “a big glass house.”<sup>318</sup> If US infrastructure owners and operators cannot defend their systems against attack, the president may be reluctant to use cyber weapons abroad, even if doing so might otherwise offer enormous benefits for conflict termination. In short: US leaders may be self-deterred from taking actions that they may need to employ. Developing emergency orders and implementation plans to protect grid reliability could reduce these glass house constraints and widen the range of options available for the president to protect US interests.

Improving grid defenses could also help strengthen the credibility of US commitments to defend key allies. Former US defense and intelligence officials have proposed that the United States and other high-cyber-capability NATO allies provide extended deterrence against cyber attacks for less capable alliance members.<sup>319</sup> But glass house concerns would call into question the credibility such commitments. Measures to strengthen grid resilience could help convince adversaries that the United States is willing to help allies respond to cyber attacks on their infrastructure.

Yet, nothing requires the United States to respond to such attacks with cyber weapons alone. On the contrary: the *National Security Strategy* and other policy documents leave open the possibility that

if cyber attacks at home or abroad are sufficiently severe, the United States will respond with conventional or even nuclear weapons. James Lewis notes that “opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return,” and will surely weigh that risk given “the immense capacity of the United States to inflict punishment” on attackers.<sup>320</sup> Emergency orders to protect the flow of power to defense installations can and should reinforce the certainty of that punishment.

But any first use of cyber weapons by the United States would entail escalatory dangers as well. If the United States were to initiate the use of destructive cyber weapons to defend US allies and interests, potential adversaries such as Russia could respond with conventional or nuclear forces. Moreover, conflicts that begin with the large-scale use of cyber weapons could also spiral out of control in ways that neither side desires or anticipates.<sup>321</sup> These escalatory risks must be in the forefront of calculations on whether and how to engage in cyber warfare. Indeed, as government agencies partner with power companies to build resilience for grid security emergencies, deterring such conflicts and reducing the likelihood of cyberwarfare should always be our prime objective.

<sup>317</sup> DOD, *Cyber Strategy*, 5.

<sup>318</sup> Schwartz, “Sen. Tillis: We Are Living in a Glass House.” For additional analysis of the glass house syndrome and its effects on constraining US options, see Miller, “Cyber Deterrence”; and Rosenbach, “Living in a Glass House.”

<sup>319</sup> Kramer, Butler, and Lotrionte, *Cyber, Extended Deterrence, and NATO*, 1.

<sup>320</sup> Lewis, *Rethinking Cybersecurity*, 9, 29. The author also argues that even if attacks on the grid occur, they would be unlikely to achieve the strategic effects that adversaries will seek, further reducing the likelihood of such attacks (see pp. 21 and 24–26).

<sup>321</sup> Danzig, *Surviving on a Diet of Poisoned Fruit*, 25; Lin, “Escalation Dynamics,” 52; and Miller and Fontaine, *A New Era*, 18–20.



## Bibliography

- 6 U.S.C. § 124l. <https://www.law.cornell.edu/uscode/text/6/124l>.
- 15 U.S.C. § 3361. <https://www.law.cornell.edu/uscode/text/15/3361>.
- 15 U.S.C. § 3363. <https://www.law.cornell.edu/uscode/text/15/3363>.
- 15 U.S.C. § 3364. <https://www.law.cornell.edu/uscode/text/15/3364>.
- 16 U.S.C. § 824a. <https://www.law.cornell.edu/uscode/text/16/824a>.
- 16 U.S.C. § 824o. <https://www.law.cornell.edu/uscode/text/16/824o>.
- 16 U.S.C. § 824o–1. <https://www.law.cornell.edu/uscode/text/16/824o–1>.
- 18 CFR 388.113. <https://www.law.cornell.edu/cfr/text/18/388.113>.
- 47 U.S.C. § 606. <https://www.law.cornell.edu/uscode/text/47/606>.
- 50 U.S.C. Appendix §2071(c). <https://law.justia.com/codes/us/2001/title50/app/defensepr/sec2071/>.
- “About Alerts.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx>.
- “About NERC.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/AboutNERC/Pages/default.aspx>.
- “About NSTAC.” DOS (US Department of State). Last published June 20, 2016. <https://www.dhs.gov/about-nstac>.
- “About 60% of the U.S. Electric Power Supply Is Managed by RTOs.” US Energy Information Administration. April 4, 2011. <https://www.eia.gov/todayinenergy/detail.php?id=790>.
- “Alert (ICS-ALERT-14-281-01E): Ongoing Sophisticated Malware Campaign Compromising ICS (Update E).” ICS-CERT. Originally released December 10, 2014, last revised December 9, 2016. <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.
- “Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure.” ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). February 25, 2016. <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.
- “Alert (TA17-163A): CrashOverride Malware.” US-CERT (US Computer Emergency Readiness Team). June 12, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-163A>.
- “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). October 20, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-293A>.
- “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). March 15, 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.

- ASD(EI&E) (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment). *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*. Washington, DC: DOD, July 2017. <https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf>.
- Assante, Michael, and Robert M. Lee. *The Industrial Control System Cyber Kill Chain*. Bethesda, MD: SANS Institute, October 2015. <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.
- “Automated Indicator Sharing (AIS).” US-CERT (US Computer Emergency Readiness Team). n.d. <https://www.us-cert.gov/ais>.
- Banham, Russ. “DDoS Attacks Evolve to Conscript Devices onto the IoT.” *Forbes*, February 4, 2018. <https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#4b5a43a86aaa>.
- Barnes, Julian E. “‘Warning Lights Are Blinking Red,’ Top Intelligence Officer Says of Russian Attacks.” *New York Times*, July 13, 2018. <https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html>.
- Blue Ribbon Study Panel on Biodefense (Hudson Institute). *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts—A Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*. Washington, DC: Hudson Institute, October 2015. <http://www.biodefensestudy.org/a-national-blueprint-for-biodefense>.
- Bordelon, Brendan. “Rounds Is Ready to Lead New Senate Cybersecurity Subcommittee.” *Morning Consult*, February 1, 2017. <https://morningconsult.com/2017/02/01/rounds-ready-lead-new-senate-cybersecurity-subcommittee/>.
- Brown, Jared T., and Daniel H. Else. *The Defense Production Act of 1950: History, Authorities, and Reauthorization*. Washington, DC: Congressional Research Service, July 28, 2014. <https://fas.org/sgp/crs/natsec/R43118.pdf>.
- “The Canada-U.S. Defence Relationship.” Department of National Defence and the Canadian Armed Forces. December 4, 2014, last modified February 10, 2015. <http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s>.
- Cherepanov, Anton, and Robert Lipovsky. “Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet.” *WeLiveSecurity* (ESET Blog), June 12, 2017. <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.
- “Compendium of U.S.-Canada Emergency Management Assistance Mechanisms.” Public Safety Canada. October 2016, last modified March 28, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cmpndm-ntdstts-cnd-2016/index-en.aspx>.
- “Compliance - Québec.” Northeast Power Coordinating Council. n.d. <https://www.npcc.org/Compliance/Quebec/Forms/Public%20List.aspx>.
- Cowan, Gerrard. “Locked Shields 2018 Practises for Large-Scale Cyber Incident.” *Jane’s 360*, April 29, 2018. <http://www.janes.com/article/79652/locked-shields-2018-practises-for-large-scale-cyber-incident>.

- Crowe, Greg. "National Guard Preparing to Defend Cyberspace for States." *Federal News Radio*, April 16, 2018. <https://federalnewsradio.com/cyber-exposure/2018/04/national-guard-preparing-to-defend-cyberspace-for-states/>.
- "Cybersecurity." American Gas Association. n.d. <https://www.aga.org/safety/security/cybersecurity/>.
- "The Cyber Threat Framework." ODNI (Office of the Director of National Intelligence). n.d. <https://www.dni.gov/index.php/cyber-threat-framework>.
- Danzig, Richard. *Catastrophic Bioterrorism—What Is to Be Done?* Washington, DC: Center for Technology and National Security Policy, August 2003. [http://www.response-analytics.org/images/Danzig\\_Bioterror\\_Paper.pdf](http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf).
- . *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Washington, DC: Center for a New American Security, July 2014. [https://s3.amazonaws.com/files.cnas.org/documents/CNAS\\_PoisonedFruit\\_Danzig.pdf](https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf).
- Defense Science Board. *Task Force on Cyber Deterrence*. Washington, DC: DOD, February 2017. [https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport\\_02-28-17\\_Final.pdf](https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf).
- DHS (US Department of Homeland Security). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: DHS, December 17, 2003. <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- . *National Cyber Incident Response Plan*. Washington, DC: DHS, December 2016. [https://www.us-cert.gov/sites/default/files/ncirp/National\\_Cyber\\_Incident\\_Response\\_Plan.pdf](https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf).
- . *National Response Framework*. 3rd ed. Washington, DC: DHS, June 2016. [https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National\\_Response\\_Framework3rd.pdf](https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf).
- . *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS, 2013. <https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf>.
- . *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage*. Washington, DC: DHS, June 2017. <https://www.fema.gov/media-library/assets/documents/154058>.
- . *Strategy for Protecting and Preparing the Homeland against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*. Washington, DC: DHS, forthcoming.
- . *U.S. Department of Homeland Security Cybersecurity Strategy*. Washington, DC: DHS, May, 15, 2018. [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf).
- DiSavino, Scott, and David Sheppard. "ConEd Cuts Power to Part of Lower Manhattan Due to Sandy." *Reuters*, October 29, 2012. <https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030>.

- DOD (US Department of Defense). *Department of Defense Manual 3020.45*. Washington, DC: DOD, last updated May 23, 2017. <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>.
- . *DoD Cybersecurity Discipline Implementation Plan*. Washington, DC: DOD, amended February 2016. <http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf>.
- . *DOD Cyber Strategy*. Washington, DC: DOD, April 2015. [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).
- . *DoD Directive 3020.40: Mission Assurance (MA)*. Washington, DC: DOD, November 29, 2016. [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).
- . *Mission Assurance Strategy*. Washington, DC: DOD, April 2012. [http://policy.defense.gov/Portals/11/Documents/MA\\_Strategy\\_Final\\_7May12.pdf](http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf).
- DOE (US Department of Energy). “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40).” *Federal Register* 83, no. 7 (2018): 1176. <https://www.federalregister.gov/documents/2018/01/10/2018-00259/grid-security-emergency-orders-procedures-for-issuance>.
- . *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. Version 1.1. Washington, DC: DOE, February 2014. <https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf>.
- . *Electromagnetic Pulse Resilience Action Plan*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf>.
- . “Energy Priorities and Allocations System Regulations (RIN 1901–AB28).” *Federal Register* 76, no. 111 (2011): 33615. <https://www.gpo.gov/fdsys/pkg/FR-2011-06-09/pdf/2011-14282.pdf>.
- . *Multiyear Plan for Energy Sector Cybersecurity*. Washington, DC: DOE, March 2018. [https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20\\_0.pdf](https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf).
- . *Quadrennial Energy Review—Transforming the Nation’s Electricity System: The Second Installment of the QER*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>.
- . *Staff Report to the Secretary on Electricity Markets and Reliability*. Washington, DC: DOE, August 2017. [https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability\\_0.pdf](https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability_0.pdf).
- . *Strategic Transformer Reserve: Report to Congress*. Washington, DC: DOE, March 2017. <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.
- “DOE’s Use of Federal Power Act Emergency Authority.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use>.

- DOS (US Department of State). *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. Washington, DC: DOS, May 31, 2018. <https://www.state.gov/documents/organization/282253.pdf>.
- Dougherty, Jon. “Biggest U.S. Power Grid Operator Suffers Thousands of Attempted Cyber Attacks per Month.” *Forward Observer*, August 28, 2017. <https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/>.
- Douris, Constance. “DARPA Research Leads Grid Security Solutions.” *The Buzz* (blog), *National Interest*, January 12, 2017. <http://nationalinterest.org/blog/the-buzz/darpa-research-leads-grid-security-solutions-19044>.
- Dragos, Inc. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. Hanover, MD: Dragos, June 13, 2017. <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>.
- EEI (Edison Electric Institute). “Comments of the Edison Electric Institute.” In *Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*. February 6, 2017.
- . *Understanding the Electric Power Industry’s Response and Restoration Process*. Washington, DC: EEI, October 2016. [http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA\\_101FINAL.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf).
- EIS Council (Electric Infrastructure Security Council). *E-PRO Handbook II: Volume 1—Fuel*. Washington, DC: EIS Council, 2016. [https://www.eiscouncil.org/App\\_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf](https://www.eiscouncil.org/App_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf).
- . *E-PRO Handbook III: Black Sky Cross-Sector Coordination and Communication*. Washington, DC: EIS Council, June 2018. [https://www.eiscouncil.org/EPRO\\_Books.aspx](https://www.eiscouncil.org/EPRO_Books.aspx).
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS-ICS. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Washington, DC: NERC, March 2016. [https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_18Mar2016.pdf](https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf).
- “Electricity Information Sharing and Analysis Center.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.
- “Electric Power Transmission Reliability Standards Compliance Monitoring and Enforcement.” Régie de l’énergie Québec. n.d. <http://www.regie-energie.qc.ca/en/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html>.
- “Emergency Communications.” DHS (US Department of Homeland Security). Last published June 26, 2018. <https://www.dhs.gov/topic/emergency-communications>.
- Energy Policy Act of 2005. Public Law 109-58. *U.S. Statutes at Large* 119 (2005): 942–943. <https://www.gpo.gov/fdsys/pkg/STATUTE-119/pdf/STATUTE-119.pdf>.
- “Energy Sector Cybersecurity Preparedness.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.



- EPRI (Electric Power Research Institute). *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research*. Report 3002000796. Palo Alto, CA: EPRI, December 2013. <https://publicdownload.epri.com/PublicDownload.svc/product=000000003002000796/type=Product>.
- . *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs*. Report 3002008999. Palo Alto, CA: EPRI, September 2016. <https://www.epri.com/#/pages/product/000000003002008999/?lang=en>.
- ESCC (Electricity Subsector Coordinating Council). *Electricity Sub-Sector Coordinating Council Charter*. Washington, DC: DHS, August 5, 2013. <https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf>.
- “ESCC: Electricity Subsector Coordinating Council.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.
- “The ESCC’s Cyber Mutual Assistance Program.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1>.
- FEMA (US Federal Emergency Management Agency). *2017 Hurricane Season FEMA After-Action Report*. Washington, DC: FEMA, July 12, 2018. <https://www.fema.gov/media-library/assets/documents/167249>.
- FERC (Federal Energy Regulatory Commission). *Cyber Security Incident Reporting Reliability Standards*. 161 FERC ¶ 61,291. December 21, 2017. <https://www.ferc.gov/whats-new/comm-meet/2017/122117/E-1.pdf>.
- . *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies, Statement of Policy*. 96 FERC ¶ 61,299. September 14, 2011.
- . *Grid Resilience in Regional Transmission Organizations and Independent System Operators*. 162 FERC ¶ 61,256. 2018. <https://www.ferc.gov/CalendarFiles/20180320102618-AD18-7-000.pdf>.
- . *Order Authorizing Acquisition and Disposition of Jurisdictional Facilities*. 163 FERC ¶ 61,005. April 3, 2018. <https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf>.
- . *Order Granting Approvals in Connection with the Dissolution of the Southwest Power Pool Regional Entity*. 163 FERC ¶ 61,094. May 4, 2018. <https://www.ferc.gov/CalendarFiles/20180504141902-RR18-3-000.pdf>.
- . *Policy Statement on Matters Related to Bulk Power System Reliability*. 107 FERC ¶ 61,052. April 19, 2004. <https://www.ferc.gov/whats-new/comm-meet/041404/E-6.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833. 157 FERC ¶ 61,123. November 17, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-4.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833-A. 163 FERC ¶ 61,125. May 17, 2018. <https://www.ferc.gov/whats-new/comm-meet/2018/051718/E-2.pdf>.

- . *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*. 156 FERC ¶ 61,215. September 22, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/092216/E-4.pdf>.
- . *Revision to Electric Reliability Organization Definition of Bulk Electric System*. Order No. 743. 133 FERC ¶ 61,150. November 18, 2010. <https://www.ferc.gov/whats-new/comm-meet/2010/111810/E-2.pdf>.
- . *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*. Order No. 773-A. 143 FERC ¶ 61,053. April 18, 2013. <https://www.ferc.gov/whats-new/comm-meet/2013/041813/E-9.pdf>.
- FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation). *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*. Washington, DC: FERC, January 2016. <https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Further Joint Study Report: Planning Restoration Absent SCADA or EMS (PRASE)*. Washington, DC: FERC, June 2017. <https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Recommended Study: Blackstart Resources Availability (BRAv)*. Washington, DC: FERC, May 2018. <https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf>.
- Fischerkeller, Michael P., and Richard J. Harknett. “Deterrence Is Not a Credible Strategy for Cyberspace.” *Orbis* 61, no. 3 (2017): 381–393. <https://www.sciencedirect.com/science/article/pii/S0030438717300431>.
- Fixing America’s Surface Transportation Act, Public Law 114-94. *U.S. Statutes at Large* 129 (2015): 1773–1774. <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.
- Frankel, Alison. “Can Customers Sue Power Companies for Outages? Yes, but It’s Hard to Win.” *Reuters* (blog), November 9, 2012. <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>.
- Galloway, T. J., Sr. “Advancing Reliability and Resilience of the Grid.” Comments presented at the FERC Reliability Technical Conference, Washington, DC, July 31, 2018. <https://www.ferc.gov/CalendarFiles/20180731084251-Galloway,%20North%20American%20Transmission%20Forum.pdf>.
- Gerson, Michael S. “Conventional Deterrence in the Second Nuclear Age.” *Parameters* 39 (Autumn 2009): 32–48. <https://ssi.armywarcollege.edu/pubs/parameters/articles/09autumn/gerson.pdf>.
- Governments of the US and Canada. *Joint United States-Canada Electric Grid Security and Resilience Strategy*. Washington, DC: The White House, December 2016. [https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint\\_US\\_Canada\\_Grid\\_Strategy\\_06Dec2016.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf).
- GWU (George Washington University) Center for Cyber and Homeland Security. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: GWU, October 2016. <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf>.
- Healy, Jason. *The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities*. SSRN, June 2016. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2836206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206).

- Homeland Security Advisory Council. *Final Report of the Cybersecurity Subcommittee: Part I—Incident Response*. Washington, DC: DOS, June 2016. <https://www.hsd.org/?view&did=794271>.
- ICF. *Assessment of Large Power Transformer Risk Mitigation Strategies*. Fairfax, VA: ICF, October 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf>.
- . *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. Fairfax, VA: ICF, June 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>.
- “Increasing Electricity Cooperation in North America.” DOE (US Department of Energy). January 11, 2017. <https://www.energy.gov/policy/articles/increasing-electricity-cooperation-north-america>.
- INL (Idaho National Laboratory). *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*. Idaho Falls, IN: INL, January 2016. <https://inldigitallibrary.inl.gov/sites/STI/STI/INL-EXT-15-35582.pdf>.
- ISO-NE (ISO New England). *Operational Fuel-Security Analysis*. Holyoke, MA: ISO-NE, January 17, 2018. [https://www.iso-ne.com/static-assets/documents/2018/01/20180117\\_operational\\_fuel-security\\_analysis.pdf](https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf).
- . “Response of ISO New England Inc.” *Response to Grid Resilience in Regional Transmission Organization and Independent System Operators* (AD18-7-000). March 9, 2018. [https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7\\_iso\\_response\\_to\\_grid\\_resilience.pdf](https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7_iso_response_to_grid_resilience.pdf).
- Jenkins, Brian Michael. “Countering al-Qaeda: The Next Phase in the War.” *The RAND Blog*, September 8, 2002. <https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html>.
- Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*. Joint Publication 1. Washington, DC: Joint Chiefs of Staff, July 12, 2017. [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1\\_ch1.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf).
- Joint Commenters. “Comments of American Public Power Association, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group.” In *Response to RIN 1901-AB40*. February 23, 2017. <http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf>.
- Kaften, Cheryl. “DoD Tests Energy Continuity with ‘Islanded’ Microgrid.” *Energy Manager Today*, April 5, 2017. <https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/>.
- Kappenman, John. *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*. Goleta, CA: Metatech, January 2010. [https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc\\_meta-r-319.pdf](https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf).
- “Key Players.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>.
- Kissane, Carolyn, and Emily Medina. “Energy Aftershocks in Store after Seismic Mexican Election.” *The Hill*, July 3, 2018. <http://thehill.com/opinion/energy-environment/395383-energy-aftershocks-in-store-after-seismic-mexican-election>.

- Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte. *Cyber, Extended Deterrence, and NATO*. Washington, DC: Atlantic Council, May 2016. [http://www.atlanticcouncil.org/images/publications/Cyber\\_Extended\\_Deterrence\\_and\\_NATO\\_web\\_0526.pdf](http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf).
- Lawrence, Bill, Charlotte de Seibert, and Philip Daigle. "E-ISAC Update." Presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, FL, March 6–7, 2018. <https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf>.
- Lazar, Jim. *Electricity Regulation in the US: A Guide*. 2nd ed. Montpelier, VT: Regulatory Assistance Project, June 2016. <http://www.raponline.org/wp-content/uploads/2016/07/rap-lazar-electricity-regulation-US-june-2016.pdf>.
- Lewis, James A. "North Korea and Cyber Catastrophe—Don't Hold Your Breath." *38 North*, January 12, 2018. <http://www.38north.org/2018/01/jalewis011218/>.
- . *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Washington, DC: CSIS, January 2018. [http://espas.eu/orbis/sites/default/files/generated/document/en/180108\\_Lewis\\_ReconsideringCybersecurity\\_Web.pdf](http://espas.eu/orbis/sites/default/files/generated/document/en/180108_Lewis_ReconsideringCybersecurity_Web.pdf).
- Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. [http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06\\_Issue-3/Fall12.pdf](http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-3/Fall12.pdf).
- Lucas, Todd. "Conservative Operations." Presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, CO, September 18–19, 2013. <http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf>.
- Lynch, Justin. "How the Russian Government Allegedly Attacks the American Electric Grid." *Fifth Domain*, July 24, 2018. <https://www.fifthdomain.com/critical-infrastructure/2018/07/24/how-the-russian-government-attacks-the-american-electric-grid/>.
- Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (Sept./Oct. 2010). <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.
- "Maritime Forces Pacific." Royal Canadian Navy. Last modified November 24, 2016. <http://www.navy-marine.forces.gc.ca/en/about/structure-marpac-home.page>.
- Marks, Joseph. "DHS Stands up New Cyber Risk Center to Protect High-Value Targets." *Nextgov*, July 31, 2018. <https://www.nextgov.com/cybersecurity/2018/07/dhs-stands-new-cyber-risk-center-protect-high-value-targets/150179/>.
- Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn. *Power Begins at Home: Assured Energy for U.S. Military Bases*. Reston, VA: Noblis, January 12, 2017. [http://www.pewtrusts.org/~media/assets/2017/01/ce\\_power\\_begins\\_at\\_home\\_assured\\_energy\\_for\\_us\\_military\\_bases.pdf](http://www.pewtrusts.org/~media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf).
- McElwee, Steven. "Probabilistic Cluster Ensemble Evaluation for Unsupervised Intrusion Detection." Unpublished thesis, Nova Southeastern University, forthcoming.



- McElwee, Steven, Jeffrey Heaton, James Fraley, and James Cannady. "Deep Learning for Prioritizing and Responding to Intrusion Detection Alerts." In *2017 IEEE Military Communications Conference Proceedings*. Piscataway, NJ: IEEE, 2017. <https://ieeexplore.ieee.org/document/8170757/>.
- McGhee, Michael. "EEI Executive Advisory Committee." Slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017. [http://www.asaie.army.mil/Public/ES/oei/docs/EEI\\_Exec-Committee.pdf](http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf).
- Miller, James N. "Cyber Deterrence Cannot Be One Size Fits All." *Cipher Brief*, August 3, 2017. [https://www.thecipherbrief.com/column\\_article/cyber-deterrence-cannot-be-one-size-fits-all-1092](https://www.thecipherbrief.com/column_article/cyber-deterrence-cannot-be-one-size-fits-all-1092).
- Miller, James N., and James R. Gosler. "Memorandum for the Chairman, Defense Science Board" (preamble). In *Task Force on Cyber Deterrence*. Washington, DC: Defense Science Board, February 2017. <http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>.
- Miller, James N., Jr., and Richard Fontaine. *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict*. Washington, DC: CNAS, September 2017. <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Project Pathways-Finalb.pdf?mtime=20170918101505>.
- Miller, Rich. "Con Edison Shuts off Power in Lower Manhattan." *DataCenter Knowledge*, October 29, 2012. <http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutdown>.
- MISO (Midcontinent Independent System Operator). *Geomagnetic Disturbance Operations Plan*. SO-P-AOP-01 Rev: 1. Carmel, IN: MISO, June 9, 2017. [https://old.misoenergy.org/\\_layouts/miso/ecm/redirect.aspx?id=252214](https://old.misoenergy.org/_layouts/miso/ecm/redirect.aspx?id=252214).
- . "MISO January 17–18 Maximum Generation Event Overview." Slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018. <https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf>.
- Mitchell, A. Weiss. "The Case for Deterrence by Denial." *American Interest*, August 12, 2015. <https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/>.
- "M-1 Reserve Margin." NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.
- Murauskaite, Egle. "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment." *38 North*, September 12, 2014. <http://www.38north.org/2014/09/emurauskaite091214/>.
- Nakashima, Ellen. "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks." *Washington Post*, July 8, 2017. [https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47\\_story.html](https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html).
- NARUC (National Association of Regulatory Utility Commissioners). *Cybersecurity: A Primer for State Utility Regulators*. Version 3.0. Washington, DC: NARUC, January 2017. <https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F>.



- . *Resolution on Physical Security*. Washington, DC: NARUC, July 16, 2014. <https://pubs.naruc.org/pub.cfm?id=53A0CAA5-2354-D714-5127-E0C411BAD460>.
- NASEO (National Association of State Energy Officials). “Comments of the National Association of State Energy Officials.” In *Response to RIN 1901–AB40*. [https://www.naseo.org/Data/Sites/1/naseo-comments\\_rin-1901%E2%80%93ab40.pdf](https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901%E2%80%93ab40.pdf).
- NATF (North American Transmission Forum). *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—A Spare Tire Approach*. Charlotte, NC: NATF, 2017. <http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf>.
- . *North American Transmission Forum External Newsletter*. Charlotte, NC: NATF, January 2018. <https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf>.
- National Defense Authorization Act for Fiscal Year 2017. Public Law 114-328. *U.S. Statutes at Large* 130 (2016): 2685–2687. <https://www.gpo.gov/fdsys/pkg/PLAW-114publ328/pdf/PLAW-114publ328.pdf>.
- NERC (North American Electric Reliability Corporation). *BAL-002-2(i)—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. Washington, DC: NERC, January 1, 2018. [https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2\(i\).pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2(i).pdf).
- . *CIP-014-2—Physical Security*. Washington, DC: NERC, October 2, 2015. <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.
- . *EOP-010-1—Geomagnetic Disturbance Operations*. Washington, DC: NERC, June 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States).
- . *EOP-011-1—Emergency Operations*. Washington, DC: NERC, April 1, 2017. [https://www.nerc.com/\\_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).
- . *Glossary of Terms Used in NERC Reliability Standards*. Washington, DC: NERC, last updated July 3, 2018. [https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary\\_of\\_Terms.pdf](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf).
- . *Grid Security Exercise: GridEx III Report*. Atlanta, GA: NERC, March 2016. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.
- . *Grid Security Exercise GridEx IV: Lessons Learned*. Atlanta, GA: NERC, March 28, 2018. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf>.
- . *History of NERC*. Washington, DC: NERC, August 2013. <http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf>.
- . *Hurricane Harvey Event Analysis Report*. Washington, DC: NERC, March 2018. [https://www.nerc.com/pa/rrm/ea/Hurricane\\_Harvey\\_EAR\\_DL/NERC\\_Hurricane\\_Harvey\\_EAR\\_20180309.pdf](https://www.nerc.com/pa/rrm/ea/Hurricane_Harvey_EAR_DL/NERC_Hurricane_Harvey_EAR_20180309.pdf).

- . “Informational Filing on the Definition of ‘Adequate Level of Reliability.’” Filing to the Federal Energy Regulatory Commission. May 10, 2013. [https://www.nerc.com/pa/Stand/Resources/Documents/Adequate\\_Level\\_of\\_Reliability\\_Definition\\_\(Informational\\_Filing\).pdf](https://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf).
- . *IRO-008-2—Reliability Coordinator Operational Analysis and Real-Time Assessments*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/IRO-008-2.pdf>.
- . *PRC-010-2—Under Voltage Load Shedding*. Washington, DC: NERC, April 2, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States).
- . *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*. Atlanta, GA: NERC, December 13, 2017. [https://www.nerc.com/comm/OC\\_Reliability\\_Guidelines\\_DL/Gas\\_and\\_Electrical\\_Operational\\_Coordination\\_Considerations\\_20171213.pdf](https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Gas_and_Electrical_Operational_Coordination_Considerations_20171213.pdf).
- . *Reliability Terminology*. Atlanta, GA: NERC, August 2013. <https://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf>.
- . *Short-Term Special Assessment: Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation*. Atlanta, GA: NERC, May 2016. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric\\_Final.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric_Final.pdf).
- . *Standard PRC-006-3—Automatic Underfrequency Load Shedding*. Washington, DC: NERC, October 1, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States).
- . *Technical Report Supporting Definition of Adequate Level of Reliability*. Washington, DC: NERC, March 26, 2013. <https://www.nerc.com/comm/Other/Pages/Adequate%20Level%20of%20Reliability%20Task%20Force%20ALRTF.aspx>.
- . *TOP-001-3—Transmission Operations*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-001-3.pdf>.
- . *TPL-007-1—Transmission System Planned Performance for Geomagnetic Disturbance Events*. Washington, DC: NERC, December 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States).
- . *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power Phase II: A Vulnerability and Scenario Assessment for the North American Bulk Power System*. Atlanta, GA: NERC, May 2013. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC\\_PhaseII\\_FINAL.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf).
- . *2016 Long-Term Reliability Assessment*. Atlanta, GA: NERC, December 2016. <https://www.nerc.com/pa/rapa/ra/reliability%20assessments%20dl/2016%20long-term%20reliability%20assessment.pdf>.
- . *VAR-001-4.2—Voltage and Reactive Control*. Washington, DC: NERC, September 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/VAR-001-4.2.pdf>.

- NERC (North American Electric Reliability Corporation) Steering Group. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* Princeton, NJ: NERC, July 13, 2014. [https://www.nerc.com/docs/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](https://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC (North American Electric Reliability Corporation) System Protection and Control Subcommittee. *Reliability Fundamentals of System Protection*. Princeton, NJ: NERC, December 2010. [https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals\\_Approved\\_20101208.pdf](https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals_Approved_20101208.pdf).
- NETL (National Energy Technology Laboratory). *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units—Volume I: The Critical Role of Thermal Units during Extreme Weather Events*. Washington, DC: DOE, March 13, 2018. <https://www.netl.doe.gov/research/energy-analysis/search-publications/vuedetails?id=2594>.
- Newman, Lily Hay. “Hacker Lexicon: What Is the Attribution Problem?” *Wired*, December 24, 2016. <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.
- NIAC (National Infrastructure Advisory Council). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. Washington, DC: NIAC, August 2017. <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>.
- Nielsen, Kirstjen M. “National Cybersecurity Summit Keynote Speech.” DHS (Department of Homeland Security). Released July 31, 2018. <https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech>.
- “NOAA Space Weather Scales.” NOAA. April 2011. <https://www.swpc.noaa.gov/sites/default/files/images/NOAAscales.pdf>.
- “North America.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/Canada.aspx>.
- “The North Atlantic Treaty.” North Atlantic Treaty Organization. April 4, 1949 (as amended). [https://www.nato.int/cps/ic/natohq/official\\_texts\\_17120.htm](https://www.nato.int/cps/ic/natohq/official_texts_17120.htm).
- Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016/2017): 44–71. [https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\\_a\\_00266](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266).
- Obama, Barack. *Executive Order—Assignment of National Security and Emergency Preparedness Communications Functions*. Washington, DC: The White House, July 6, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness->.
- . *Executive Order—Coordinating Efforts to Prepare the Nation for Space Weather Events*. Washington, DC: The White House, October 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events>.
- . *Executive Order—Improving Critical Infrastructure Cybersecurity*. Executive Order 13636. Washington, DC: The White House, February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

- . *Executive Order—National Defense Resources Preparedness*. Washington, DC: The White House, March 16, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/03/16/executive-order-national-defense-resources-preparedness>.
- . *United States Cyber Incident Coordination*. Presidential Policy Directive 41. Washington, DC: The White House, July 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
- ODNI (Office of the Director of National Intelligence). *A Common Threat Framework: A Foundation for Communication*. McLean, VA: ODNI, January 26, 2018.
- Orenstein, Daniel G., and Lexi C. White. *Emergency Declaration Authorities across All States and D.C.* Edina, MN: Network for Public Health Law, June 16, 2015. [https://www.networkforphl.org/\\_asset/gxrdwm/Emergency-Declaration-Authorities.pdf](https://www.networkforphl.org/_asset/gxrdwm/Emergency-Declaration-Authorities.pdf).
- Paradise, Theodore J., et al. “ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance—RIN 1901–AB40.” Email to Jeffrey Baumgartner, US Department of Energy, February 6, 2017. [http://www.isorto.org/Documents/Report/20170206\\_Final\\_IRC-DOE\\_NOPR\\_Comments\\_re\\_Grid\\_Security\\_Emergency.pdf](http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf).
- Parfomak, Paul W. *Pipelines: Securing the Veins of the American Economy, Testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*. Washington, DC: Congressional Research Service, April 19, 2016. <http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf>.
- Parfomak, Paul W., Richard J. Campbell, Robert Pirog, Michael Ratner, Phillip Brown, John Frittelli, and Marc Humphries. *Cross-Border Energy Trade in North America: Present and Potential*. Washington, DC: Congressional Research Service, January 30, 2017. <https://fas.org/sgp/crs/misc/R44747.pdf>.
- Perry, Richard (US secretary of energy). Letter to the Federal Energy Regulatory Commission. September 28, 2017. <https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf>.
- Phillips, Tony. “Solar Shield—Protecting the North American Power Grid.” *NASA Science*, October 26, 2010. [https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\\_solarshield](https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield).
- PJM. “Comments and Responses of PJM Interconnection, L.L.C.” In *Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000). March 9, 2018. <http://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx>.
- . “Conservative Operations.” Training materials presented on January 27, 2015. <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.
- . *PJM Manual 13: Emergency Operations*. Rev. 65. Audubon, PA: PJM, January 1, 2018. <http://www.pjm.com/~/-/media/documents/manuals/m13.ashx>.



- Puryear, Cotton. "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade." *National Guard*, September 19, 2017. <http://www.nationalguard.mil/News/Article/1315685/91st-cyber-brigade-activated-as-army-national-guards-first-cyber-brigade/>.
- Reagan, Ronald. "The President's News Conference." August 12, 1986. Transcript. The American Presidency Project, Gerhard Peters and John T. Woolley. <http://www.presidency.ucsb.edu/ws/?pid=37733>.
- "Reliability Coordinators." NERC (North American Electric Reliability Corporation). As of June 1, 2015. <https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.
- "REMEDYS: Research Exploring Malware in Energy Delivery Systems." Cyber Resilient Energy Delivery Consortium. March 26, 2018. <https://cred-c.org/researchactivity/remedys-research-exploring-malware-energy-delivery-systems>.
- "The Role of Microgrids in Helping to Advance the Nation's Energy System." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/role-microgrids-helping>.
- "Roles and Responsibilities of Governments in Natural Resources." Natural Resources Canada. Last modified October 2, 2017. <http://www.nrcan.gc.ca/mining-materials/taxation/8882>.
- Rosenbach, Eric. "Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks." *Prepared Statement for the United States Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*. June 12, 2017. [https://www.foreign.senate.gov/imo/media/doc/061317\\_Rosenbach\\_Testimony.pdf](https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf).
- "Sandia's Grid Modernization Program Newsletter." Sandia National Laboratories. December 2017. <https://content.govdelivery.com/accounts/USDOESNLEC/bulletins/1c11ce6>.
- Schwartz, Ian. "Sen. Tillis: We Are Living in a Glass House Throwing Rocks Complaining about Election Interference." *RealClear Politics*, January 5, 2017. [https://www.realclearpolitics.com/video/2017/01/05/sen\\_tillis\\_we\\_are\\_living\\_in\\_a\\_glass\\_house\\_throwing\\_rocks\\_complaining\\_about\\_election\\_interference.html](https://www.realclearpolitics.com/video/2017/01/05/sen_tillis_we_are_living_in_a_glass_house_throwing_rocks_complaining_about_election_interference.html).
- "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response." DOE (Department of Energy). February 14, 2018. <https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency>.
- SERC. *Conservative Operations Guidelines*. Guide-800-101. Charlotte, NC: SERC, May 20, 2015. [https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines\\_rev-0-\(05-20-15\).pdf?sfvrsn=2](https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2).
- Severe Impact Resilience Task Force. *Severe Impact Resilience: Considerations and Recommendations*. Washington, DC: NERC, May 9, 2012. [https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF\\_Final\\_May\\_9\\_2012-Board\\_Accepted.pdf](https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf).



- Shelton, William L. "Threats to Space Assets and Implications for Homeland Security." *Written Testimony before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*. March 29, 2017. <http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf>.
- Sistrunk, Chris. "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)." *SANS Industrial Control Systems Security Blog*, January 8, 2016. <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>.
- Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (Winter 2016/17): 73–109. [https://www.mitpressjournals.org/doi/10.1162/ISEC\\_a\\_00267](https://www.mitpressjournals.org/doi/10.1162/ISEC_a_00267).
- Smith, Rebecca. "U.S. Officials Push New Penalties for Hackers of Electrical Grid." *Wall Street Journal*, August 5, 2018. <https://www.wsj.com/articles/u-s-officials-push-new-penalties-for-hackers-of-electrical-grid-1533492714>.
- Smith, Scott S. "Roles and Responsibilities for Defending the Nation from Cyber Attack." *Testimony Before the Senate Armed Services Committee*. October 19, 2017. <https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities>.
- Sobczak, Blake, Hannah Northey, and Peter Behr. "Cyber Raises Threat against America's Energy Backbone." *Energy Wire*, May 23, 2017. <https://www.eenews.net/stories/1060054924/>.
- Social Media Working Group for Emergency Services and Disaster Management. *Countering False Information on Social Media in Disasters and Emergencies*. Washington, DC: DHS, March 2018. [https://www.dhs.gov/sites/default/files/publications/SMWG\\_Countering-False-Info-Social-Media-Disasters-Emergencies\\_Mar2018-508.pdf](https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf).
- "Spare Transformers." EEI (Edison Electric Institute). n.d. <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.
- Stanley, Andrew J. *Mapping the U.S.-Canada Energy Relationship*. Washington, DC: CSIS, May 2018. [https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507\\_Stanley\\_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507_Stanley_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz).
- "State and Local Energy Assurance Planning." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/energy-assurance/emergency-preparedness/state-and-local-energy-assurance-planning>.
- State of New Jersey Board of Public Utilities. *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196). March 18, 2016. <http://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf>.
- Stockton, Paul. On behalf of Exelon Corporation. *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*. Docket No. RM18-1-000. October 23, 2017.
- . "Thresholds and Criteria for Declaring Grid Security Emergencies." Study for the US Department of Energy. January 31, 2018.

- Sukumar, Arun M. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare* (blog), July 4, 2017. <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.
- "Transmission Equipment Ready When Needed." Grid Assurance. n.d. <http://www.gridassurance.com/equipment-subscribers/>.
- Trump, Donald. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Executive Order 13800. Washington, DC: The White House, May 11, 2017. <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
- Ucci, Daniele, Leonardo Aniello, and Roberto Baldoni. "Survey on the Usage of Machine Learning Techniques for Malware Analysis." *ACM Transactions on the Web* 1, no. 1 (October 2017): 1:1–1:34. <https://pdfs.semanticscholar.org/d310/47e426b8b5c2aa52108899a800bedd966f07.pdf>.
- "United States Mandatory Standards Subject to Enforcement." NERC. n.d. <https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States>.
- U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington, DC: DOE, April 2004. <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.
- US Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington, DC: US Cyber Command, released March 2018. <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>.
- Van Broekhoven, S. B., N. Judson, S. V. T. Nguyen, and W. D. Ross. *Microgrid Study: Energy Security for DoD Installations*. Technical Report 1164. Lexington, MA: MIT, June 2012. <https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf>.
- Vine, Doug. *Interconnected: Canadian and U.S. Electricity*. Arlington, VA: Center for Climate and Energy Solutions, March 2017. <https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf>.
- Walker, Bruce J. *Written Testimony before the U.S. Senate Committee on Energy and Natural Resources*. March 1, 2018. [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=1C574731-A9C0-4E1C-9E05-15C492E332B1](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1).
- Weiss, Walter. "Rapid Attack Detection, Isolation and Characterization Systems (RADICS)." Defense Advanced Research Projects Agency. n.d. <https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems>.
- Western Electricity Coordinating Council. "Conservative System Operations." Training slides. n.d. <http://docplayer.net/55224883-Conservative-system-operations.html>.
- The White House. *National Security Strategy of the United States of America*. Washington, DC: The White House, December 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- "Work Continues on ITC Lake Erie Project." *Transmission Hub*, February 19, 2018. <https://www.transmissionhub.com/articles/2018/02/work-continues-on-itc-lake-erie-project.html>.



## Acknowledgments

My special thanks go to Robert Denaburg, senior analyst at Sonecon LLC. I also thank the following colleagues for helpful reviews of this study: Michael Assante (SANS Institute); Wayne Austad (Idaho National Laboratory); Terry Boston; Stuart Brindley; Gerry Cauley; Richard Danzig (JHU/APL); Daniel Elmore (Idaho National Laboratory); Peter Grandgeorge (Berkshire Hathaway Energy); Emily Goldman (US Cyber Command); Sean Griffin (ecubed us LLC); Dave Halla (JHU/APL); Jon Jipping (ITC Holdings); Debra Lavoy (Narrative Builders); Bill Lawrence (NERC); Joseph Maurio (JHU/APL); James Miller (JHU/APL); Michael Moskowitz (JHU/APL); Richard Mroz; Steven T. Naumann (Exelon Corporation); Catherine Peacock (JHU/APL); Emilia Probasco (JHU/APL); Erin Richardson (JHU/APL); David Roop (Dominion Energy); Matthew Schaffer (JHU/APL); senior leaders at Southern Company; Kyle Thomas (Dominion Virginia Power); and Virginia Wright (Idaho National Laboratory). I also thank the many additional industry and government reviewers who preferred to remain anonymous.

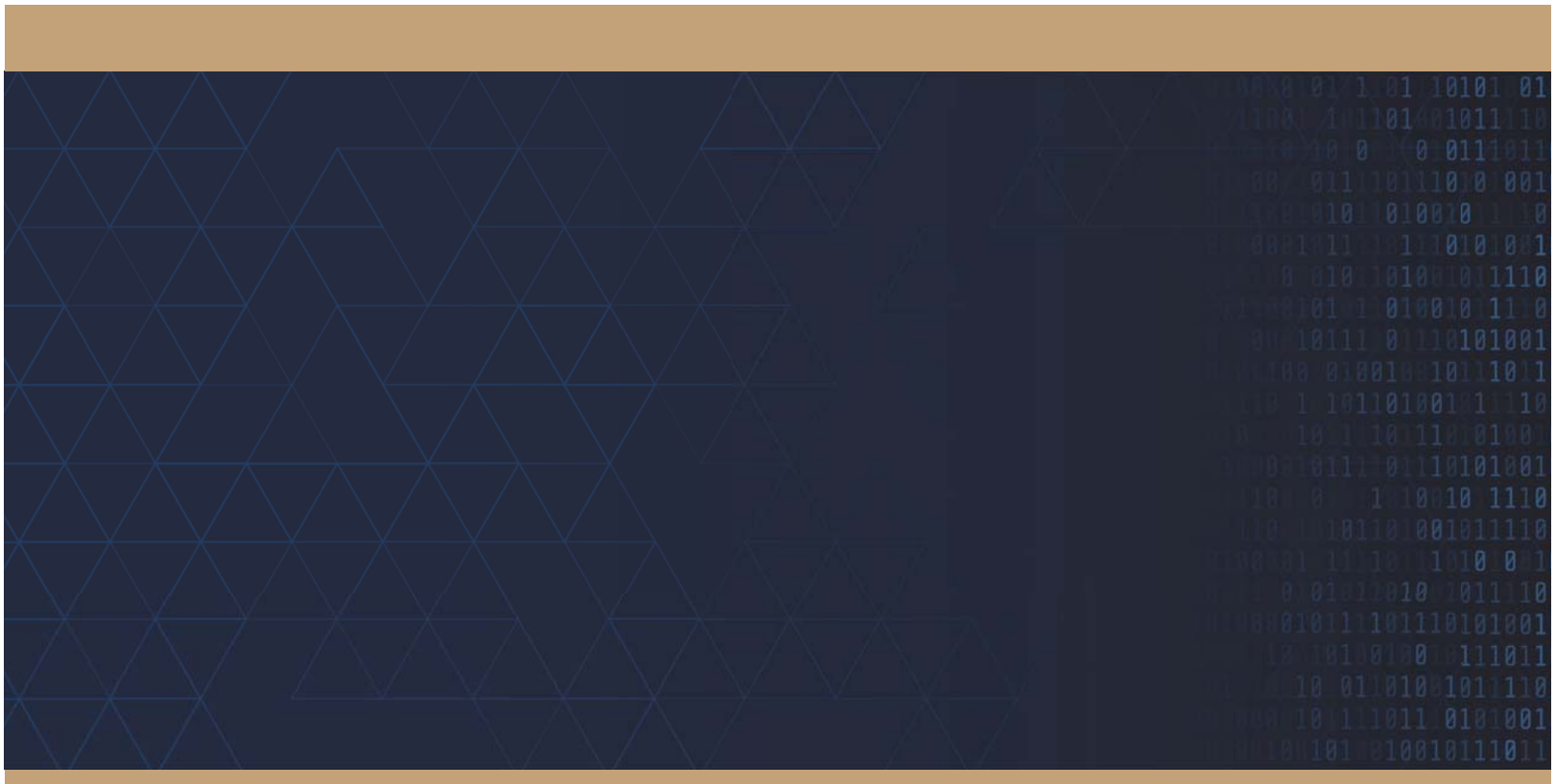
## About the Author

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC, and a senior fellow of JHU/APL. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support in Superstorm Sandy and other disasters. Dr. Stockton also served as the Department of Defense (DOD) domestic crisis manager and was responsible for defense critical infrastructure protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors and was responsible for developing and overseeing the implementation of DOD security policy in the Western Hemisphere. Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation, associate provost of the Naval Postgraduate School, and director of the school's Center for Homeland Defense and Security. Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the author of *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System* (Laurel, MD: JHU/APL, 2016) and numerous other publications. He served as the facilitator of the GridEx IV exercise (November 2017) and is a member of the Homeland Security Advisory Council and other public and private sector boards.









**To:** Joe McClelland

**Through:** (b) (6), David Andrejcak, Harry Tom

**From:** (b) (6)

**Subject:** Summary of “Enhancing the Resilience of the Nation’s Electricity System”

**Date:** March 20, 2018

**I. Introduction**

(b) (5)

[Redacted text block]

(b) (5)

**II. Summary of Study Report**

(b) (5)

[Redacted text block]

[Redacted text block]

[Redacted text block]

---

<sup>1</sup> Available at <http://nap.edu/24836>

(b) (5)



(b) (5)

A large rectangular area of the document is completely redacted with a solid black box. The redaction covers approximately the top third of the page content.A large rectangular area of the document is completely redacted with a solid black box. This redaction covers the middle section of the page, below the first redacted block.A large rectangular area of the document is completely redacted with a solid black box. This redaction covers the bottom section of the page, below the second redacted block.



(103). Recommendation 5.5 is for the DOE and DHS to “evaluate and recommend the  
(b) (5)

[Redacted]

[Redacted]

[Redacted]

(b) (5)

(b) (5) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

(b) (5) [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (5) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



(b) (6)

**From:** Jim Vess <jvess@euci.com>  
**Sent:** Friday, February 23, 2018 4:27 PM  
**To:** (b) (6)  
**Subject:** Physical and Cyber Security for Utilities symposium  
**Attachments:** 0418-energy-security.pdf

(b) (6),

**I hope you don't mind my forwarding you this email regarding the upcoming *Physical and Cyber Security for Utilities* symposium that I thought would be of interest either to yourself or your colleagues. I would appreciate any feedback you might have regarding the program. The symposium is scheduled for April 3-4, 2018 in Denver, CO.**

**Continuing Education: EUCI is authorized to offer 1.0 [IACET CEUs](#) for this event. [Click here](#) for a list of some of the organizations that accept the IACET CEU.**

**Symposium Overview:**

Physical and Cyber Security for Utilities gives plant managers, plant operators, heads of physical, cyber and corporate security a full understanding of what is at stake when it comes to securing their plant and how they can ensure the safety and security of their operations. The symposium will cover the role of power generation plants and T&D facilities as part of the nation's critical infrastructure. Attendees will learn to recognize the external drivers and regulatory requirements for plant physical security. They will learn to organize their plants and substations for cyber and physical security as well as safety. Attention will be paid to how to assess and upgrade a facility's current security organization. Experts will review how to apply cyber security guidelines and advanced technologies for power generation and transmission security programs. Finally, there will be a "utilities Q&A" so attendees can ask their own questions of how utilities are handling their security protocols.

**NOTE: The early bird rate for these events ends Friday, March 16th, be sure to register by this date to receive the Early Bird rate.**

I have attached the event brochure which include a detailed agenda and registration/hotel information can be found on the last page.

I appreciate your forwarding along to anyone who would have an interest.

If you have any questions regarding this program, would like to discuss any special pricing, if you would like to register over the phone, or need the early bird rate extended, please feel free to contact me at **720-988-1253** or via email at [jvess@euci.com](mailto:jvess@euci.com). You can also register online at: [https://www.euci.com/event\\_post/0418-energy-security/?x=29157v1Lx0101&rf=Jim](https://www.euci.com/event_post/0418-energy-security/?x=29157v1Lx0101&rf=Jim)

We hope you will be able to attend.  
Thank you for your time,

**Jim Vess**  
Marketing Coordinator



direct 720-988-1253 | main 303-770-8800 | [jvess@euci.com](mailto:jvess@euci.com)

For a list of upcoming events, please visit [www.euci.com](http://www.euci.com)

Follow Us





---

This information contained in this email and any attachments may contain confidential and/or privileged material and is the sole property of EUCL. It is intended solely for the person(s) to which it is addressed. Any review, retransmission, dissemination, or taking of any action in reliance upon this information by persons or entities other than the intended recipient(s) is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

# PHYSICAL AND CYBER SECURITY FOR UTILITIES: *Protecting Generation and Transmission Facilities*

April 3-4, 2018

Courtyard by Marriott Denver Cherry Creek  
Denver, CO

## POST-CONFERENCE WORKSHOP

### **CIP-014 Compliance: Protecting the Power Grid from Physical Attack**

WEDNESDAY, APRIL 4, 2018

“

*“I am usually reluctant to attend a 1 and a half day conference, but the information provided was excellent. Totally worth my time.”*

Manager of Safety & Security, East Kentucky  
Power Cooperative



TAG US #EUCIEvents  
FOLLOW US @EUCIEvents



EUCI is authorized by  
IACET to offer 1.0 CEUs for  
the conference and 0.4  
CEUs for the workshop.

# OVERVIEW

Power companies today face unprecedented challenges when it comes to both physical and cyber security. Given the immense amount of power generated and critical role power generation and transmission facilities play in the nation's infrastructure, the cost of a security breach goes beyond mere financial damage – it can affect the safety of an entire region. For this reason alone, it is imperative for utilities and plant managers to initiate effective security protocols within their operating budgets.

Cyber security attacks on infrastructure targets are happening with increased sophistication and frequency. Each power generation site has a complicated collection of controls that may include both legacy systems and smart assets. Each system presents challenges that range from patching to the introduction of an entire array of not-well-understood vulnerabilities. Many plants are old, and upgrading them is more than a simple matter of adding new technologies. Old systems may need to be replaced or upgraded as well. When new technologies are built on top of legacy systems, new risks may emerge as different systems interact. Companies are developing multi-pronged approaches to cyber security such as threat hunting, a proactive measure to protect their systems.

Physical and Cyber Security for Utilities gives plant managers, plant operators, heads of physical, cyber and corporate security a full understanding of what is at stake when it comes to securing their plant and how they can ensure the safety and security of their operations. The symposium will cover the role of power generation plants and T&D facilities as part of the nation's critical infrastructure. Attendees will learn to recognize the external drivers and regulatory requirements for plant physical security. They will learn to organize their plants and substations for cyber and physical security as well as safety. Attention will be paid to how to assess and upgrade a facility's current security organization. Experts will review how to apply cyber security guidelines and advanced technologies for power generation and transmission security programs. Finally, there will be a "utilities Q&A" so attendees can ask their own questions of how utilities are handling their security protocols.

# LEARNING OUTCOMES

- Reduce risk by securing critical infrastructure against human, physical, and cyber threats
- Examine costs and benefits of security investments
- Identify mitigation efforts that will ensure rapid recovery of plant operations in the case of security breaches
- Recognize where cyber security and physical security overlap
- Set benchmarks for intrusion detection, perimeter patrol, lighting
- Effectively upgrade security protocols when responsibilities are transferred from one department to another
- Bring older facilities up to current standards
- Explain the role power production and transmission facilities as part of the country's critical infrastructure
- Establish rapid response and recovery protocols in the case of a cyber security breach
- Define current threats to plant security based on recent incidents
- Discuss the intersection between plant safety and security
- Prepare for threats and resolve conflicts

# WHO SHOULD ATTEND

Directors of Operations, Heads of Security, Cyber and Corporate Security Managers from Power Generation and Transmission Facilities, Security Companies, Software Companies, Law Firms, and Engineering Firms.

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)





# AGENDA

TUESDAY, APRIL 3, 2018

**8:00 – 8:30 am**

## **Registration and Continental Breakfast**

**8:30 – 9:30 am**

## **Power Production and Transmission as Critical Infrastructure**

More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to various industries, households and businesses. The energy infrastructure contains more than 6,413 power plants which includes 3,273 traditional electric utilities and 1,738 nonutility power producers with approximately 1,075 gigawatts of installed generation. Electricity generated at power plants is transmitted over 203,930 miles of high-voltage transmission lines. The electricity infrastructure is highly automated and controlled by utilities and regional grid operators nationwide; therefore, it is imperative for owners and operators to collaborate and coordinate to ensure the security and resilience of the grid due to its' complex operating structure and it's critical and essential function across virtually all critical infrastructure sectors. This presentation will discuss:

- Assessing security risks and threats to power plants
- Securing critical infrastructure from all hazards
- Enhancing critical infrastructure resilience
- Sharing information to enable risk-informed decision making
- Adopting, learning, and adaptation in the face of changing conditions

***Shawn Graff, Regional Director, Region VIII, Office of Infrastructure Protection, Department of Homeland Security***

**9:30 – 10:30 am**

## **A Forward Thinking Approach for Developing a Physical and Cyber Security Plan for Low Impact Assets**

Developing a physical and cyber security plan to implement at Low Impact generation sites is an exercise in planning for current state as well as future proofing for changes in physical infrastructure and changing requirements. Existing Low Impact assets have a broad range of capabilities, risks, age in equipment, and operational considerations even within the same entity. Developing an approach to ensure consistency, operational flexibility, and reduce overall cyber and physical risk is a challenge. This presentation will look at using a risk based approach to developing a program to implement Physical and cyber security plans to support existing and future low impact sites.

- Developing a program that supports existing aging low impact assets and future development
- Using a risk assessment to identify controls based on individual sites
- Developing programs that separate controls for physical and cyber security plans
- Implementing controls that can be implemented across high, medium, and low impact assets but scaled to impact level
- Presenting an example using DTE Energy's medium and low impact generations sites implementation program

***Mike Reterstorf, IT Manager in NERC Compliance Office, DTE Energy***

**10:30 – 11:00 am**

## **Networking Break**

**11:00 – 11:45 am**

## **Assessing Plant Physical Security: The Newcomer's Perspective**

- Assessing an established organization for security risk factors
- Fortification of existing intrusion detection
- Intrusion detection and monitoring
- Policies and programs
- Integrating company culture with new initiatives

***Jason Maldonado, Security, Emergency Management & Safety Management, Platte River Power Authority***

***Justin Allar, Security Systems Supervisor, Platte River Power Authority***

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)



# AGENDA

TUESDAY, APRIL 3, 2018 (CONTINUED)

## 11:45 am – 12:30 pm **Intersections: The Overlap Between Safety and Security**

- Regulatory compliance and what drives it
  - NERC/FERC requirements
  - OSHA requirements
- Duty to protect employees
  - Threats of workplace violence
- Emergency management and incident response
  - Roles of safety professionals vs. security professionals

**Jason Maldonado, Security, Emergency Management & Safety Management, Platte River Power Authority**

**Justin Allar, Security Systems Supervisor, Platte River Power Authority**

## 12:30 – 1:30 pm **Group Luncheon**

## 1:30 – 2:30 pm **Collaborative R&D in Securing Power Generation**

The increasing sophistication and frequency of cyber security attacks on infrastructure targets is another example of the unprecedented challenges to power generators today. In response, regulations around the globe are requiring an active cyber security strategy for all power generation, significantly more complex than traditional controls network segregation (i.e. "air-gapping").

The core cyber security challenge is that each power generation site is deploying more digital Industrial Control System (ICS) assets from a variety of vendors as a result of obsolescence, and to take advantage of performance gains. These various digital systems and components are more highly integrated than ever before resulting in a larger cyber security attack surface. The rapidly evolving threat landscape and sophisticated ICSs present both a technical and organizational challenge for developing, implementing, and maintaining a successful cyber security program. On top of the numerous technical challenges, cultural and programmatic gaps need to be addressed in a consistent and coordinated approach.

EPRI's Generation Sector has been leveraging industry resources and R&D efforts in the Nuclear and Power Delivery programs to tailor research to power generation. Included in this presentation will be the following:

- NIST Level 4, decentralized hardware-based Remote Access Solution that could streamline management of interactive remote access
- Utilizing proven enterprise architecture techniques to facilitate IT/OT integration in Power Generation
- Research into real-time detection capabilities to better automate threat detection
- A new technical assessment optimization methodology that protects against emerging threats and the added costs of changing regulation

Most importantly, EPRI has been developing a community of industry peers dedicated to securing power generation. This presentation will describe how others in the industry can leverage this resource.

**Justin Thibault, Senior Technical Leader, EPRI**

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)

# AGENDA

TUESDAY, APRIL 3, 2018 (CONTINUED)

**2:30 – 3:00 pm**

## **Networking Break**

**3:00 – 4:00 pm**

## **Confronting Active Shooters in a Utility Setting: Preparing for Threats**

The presentation will provide methods on how to train and drill for an active shooter in and out of the workplace. Some topics that will be covered will include, recognizing signs of an active shooter before an incident happens, how to act on the signs, how to increase your chances for survival in a moment of crisis, and providing tips on how to conduct active shooter drills.

- Active shooter/killer trends
- Active killer response and developing the survival mentality
- Tips on how to perform an active shooter drill

***Tim Kacena, Physical Security Specialist – Investigator, Nebraska Public Power District***

**4:00 – 5:00 pm**

## **Conflict Resolution Training for Utilities**

This session covers conflict resolution in the workplace, primarily teaching how to deal with difficult customers in stressful situations to avoid escalation. Actual footage of events will be used as well as group discussion.

- What training are we giving co-workers to de-escalate dangerous situations?
- Identify stressful situations that employees could encounter
- Determine an appropriate time to contact law enforcement

***Tim Kacena, Physical Security Specialist – Investigator, Nebraska Public Power District***

**5:00 pm**

## **End of Day One**

WEDNESDAY, APRIL 4, 2018

**8:00 – 8:30 am**

## **Continental Breakfast**

**8:30 – 9:30 am**

## **Threat Hunting for Cyber Risks**

Implementing a complex layered security approach with multiple reporting tools alerting on infections and signatures is no longer an acceptable security approach. Everyone likes to use the words “proactive security” but what exactly does that mean? This talk will go over a proactive security approach known as threat hunting, how it varies from current cybersecurity practices, what it’s going to take to implement, and how threat hunting can improve your cybersecurity landscape.

- What is Threat Hunting
- Current Cyber Practices (Reactive) vs Threat Hunting (Proactive)
- Review use cases where this has occurred, where in certain environments a “hack proof” defense can be created
- What’s it going to take
  - o Analyst functions
  - o Network Analysis
  - o Host Analysis
- Is this possible in an ICS Environment?

***Fred Bonewell, Chief Safety and Security Officer, CPS Energy***

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)



# AGENDA

WEDNESDAY, APRIL 4, 2018 (CONTINUED)

**9:30 – 10:30 am**

## **Implementing Substation Physical Security Risks and Controls**

For years security departments have worked with law enforcement in response to copper thefts from substations. The Metcalf substation ballistic attack in 2013 along with other criminal and terrorist threats have brought to light substation risks and made it clear that robust physical security of substations is needed to protect against disruption of operations. At critical sites, controls must deter, detect, delay, communicate and allow for a prompt response. A defense in depth strategy is required to reduce risks and vulnerabilities associated with unauthorized access to personnel, equipment, systems and materials. This session will cover processes needed to effectively mitigate substation physical security risks:

- To effectively mitigate substation physical security risks:
- Working closely with operational functions to understand and document substations criticality to operations, and tier accordingly
- Identifying and delineating control requirements for each tier considering risks of unauthorized access to substations and operational impacts
- Assessing capital expenditures and subsequent maintenance costs
- Conducting periodic site security assessments to identify new vulnerabilities and tracking any issues that are identified until they are addressed
- Developing processes to continuously assess criminal and terrorist risks that may threaten substations and creating new risks mitigation strategies

**Mark Bullock, Director of Security, Commonwealth Edison**

**10:30 – 11:00 am**

## **Networking Break**

**11:00 am – 12:00 pm**

## **Mitigate Risk to Generation Assets through an Assessment Program**

Strategic enhancements to the existing Physical Security Assessment process can result in improved analysis of physical security application and risk management at generation facilities. This session covers an approach that was developed to deploy protection measures through corporate governance to minimize security risk.

- To effectively mitigate physical security risks
- collaborate with Business Unit and operational functions to understand and document criticality to operations, and tier accordingly
- Identify and standardize minimum Security Protection Standards as countermeasures elements of the Security Assessment process
- Implement a prototype system to facilitate proof of concept in Security Assessment performance
- Perform periodic Site Security Assessments based on tier to validate protection measures
- Determine acceptable risk tolerance level
- Develop and Implement Program Governance for a uniform methodology of performing Security Assessments to mitigate risk

**Michelle Draxton, Manager of Generation Security, Exelon Corporate and Information Security Services**

**12:00 pm**

## **Symposium Concludes**

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)

## POST-SYMPOSIUM WORKSHOP

# CIP-014 Compliance: Protecting the Power Grid from Physical Attack

WEDNESDAY, APRIL 4, 2018

**12:30 – 1:00 pm**      **Workshop Registration****1:00 – 4:00 pm**      **Workshop Timing**

## OVERVIEW

Securing the North American power grid is a top priority for both regulators and utilities. While the industry remains focused on grid resilience, physical security threats remain that could affect generation, transmission, and distribution operations. A coordinated and simultaneous attack on multiple high voltage transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts. Such an event would have serious economic and social consequences. While adversaries are becoming more informed and highly capable, we will discuss recent physical security events, NERC CIP-014 compliance, and strategies to reduce overall threats and vulnerabilities.

## LEARNING OUTCOMES

- Find out what industry is doing today to better protect critical electric infrastructure and identify emerging threats facing substations, generating plants, and energy control centers
- Implement the NERC CIP-014 standard, mitigation strategies, and effective compliance
- Recognize how utilities can incorporate deter, detect, and delay into their physical security program to meet compliance and become a “hard target”

## WORKSHOP AGENDA

**1:00 – 2:30 pm****Physical Threats to the Grid**

Participants will learn about recent physical attacks against energy infrastructure, including an in-depth analysis of the 2013 California substation shooting, which was the catalyst for the NERC CIP-014 standard. Also discussed will be how to conduct a proper threat and vulnerability assessment that will feed into a comprehensive physical security response plan.

We will Discuss:

- Physical Attack Scenarios
- The April 16, 2013 Metcalf Substation Shooting
- The Insider Threat
- Emerging Threats Including Drones and Civil Unrest

**2:30 – 3:00 pm****Coffee Break****REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)**



# WORKSHOP AGENDA

**3:00 – 5:00 pm****Deter, Detect, Delay, Assess, Communicate, and Respond Under NERC CIP-014**

Learn how to incorporate the information from a threat and vulnerability assessment and apply it to a mitigation strategy and future road map. Participants will learn specifics about the NERC-014 standard, how to achieve compliance, and ensuring you have properly protected the “crown jewels”.

We will Discuss:

- Physical Security Technologies Being Used in Industry
- How to Create a Robust Physical Security Plan
- CIP-014 R4, R5, and R6 Insights
- Engaging the Regulator and Information Sharing

**5:00 pm****Workshop Concludes**

# WORKSHOP INSTRUCTOR

**Brian Harrell****CPP, Vice President of Security, AlertEnterprise**

Brian Harrell, CPP, is the Vice President of Security at AlertEnterprise, a technology and advisory firm that provides critical infrastructure owners with consultation on physical and cybersecurity protections. He is the former Operations Director of the Electricity ISAC and Director of Critical Infrastructure Protection Programs at the North American Electric Reliability Corporation (NERC) where he was charged with helping protect North America's electric grid from physical and cyber-attack. Brian was a Standard Drafting Team (SDT) member for the NERC physical security standard, CIP-014. Brian has spent time during his career in the US Marine Corps, US Department of Homeland Security, and various private sector agencies with the goal of protecting the United States from security threats. Brian is also a Senior Fellow at The George Washington University Center for Cyber & Homeland Security (CCHS) where he provides insight and analysis on homeland security, counterterrorism, and cybersecurity issues.

**REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)**

# REQUIREMENTS FOR SUCCESSFUL COMPLETION

Participants must sign in/out each day and be in attendance for the entirety of the course to be eligible for continuing education credit.

## INSTRUCTIONAL METHODS

Powerpoint presentations and case studies will be used throughout this conference

## IACET CREDITS



EUCI has been accredited as an Authorized Provider by the International Association for Continuing Education and Training (IACET). In obtaining this accreditation, EUCI has demonstrated that it complies with the ANSI/IACET Standard which is recognized internationally as a standard of good practice. As a result of their Authorized Provider status, EUCI is authorized to offer IACET CEUs for its programs that qualify under the ANSI/IACET Standard.

**EUCI is authorized by IACET to offer 1.0 CEUs for the conference and 0.4 CEUs for the workshop.**

## EVENT LOCATION

A room block has been reserved at the Courtyard by Marriott Denver Cherry Creek, 1475 S Colorado Blvd, Denver, CO 80222, for the nights of April 2-3, 2018. Room rates are \$139 plus applicable tax. Call **1-303-757-8797** for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is March 5, 2018 but as there are a limited number of rooms available at this rate, the room block may close sooner. ***Please make your reservations early.***

## REGISTER 3, SEND THE 4TH FREE

Any organization wishing to send multiple attendees to this event may send 1 FREE for every 3 delegates registered. Please note that all registrations must be made at the same time to qualify.

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)



# REGISTRATION INFORMATION

## Mail Directly To:

EUCI  
4601 DTC Blvd., Ste. 800  
Denver, CO 80237  
OR, scan and email to: [conferences@euci.com](mailto:conferences@euci.com)

**WWW.EUCI.COM**  
**p: 303-770-8800**  
**f: 303-741-0849**

## PLEASE REGISTER

☐ **BOTH PHYSICAL AND CYBER SECURITY FOR UTILITIES AND POST- CONFERENCE WORKSHOP**

APRIL 3-4, 2018: US \$1795

Early bird on or before March 16, 2018: US \$1595

☐ **PHYSICAL AND CYBER SECURITY FOR UTILITIES ONLY**

APRIL 3-4, 2018: US \$1395

Early bird on or before March 16, 2018: US \$1195

☐ **POST-CONFERENCE WORKSHOP ONLY**

APRIL 4, 2018: US \$595

Early bird on or before March 16, 2018: US \$495

☐ I'M SORRY I CANNOT ATTEND, BUT PLEASE EMAIL ME A LINK TO THE CONFERENCE PROCEEDINGS FOR US \$395

Redacted Pursuant to FOIA Exemption 6

## EVENT LOCATION

A room block has been reserved at the Courtyard by Marriott Denver Cherry Creek, 1475 S Colorado Blvd, Denver, CO 80222, for the nights of April 2-3, 2018. Room rates are \$139 plus applicable tax. Call **1-303-757-8797** for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is March 5, 2018 but as there are a limited number of rooms available at this rate, the room block may close sooner.

**Please make your reservations early.**

## ENERGIZE WEEKLY

EUCI's Energize Weekly e-mail newsletter compiles and reports on the latest news and trends in the energy industry. Newsletter recipients also receive a different, complimentary course presentation every week on a relevant industry topic. The presentations are selected from a massive library of more than 1,000 current presentations that EUCI has gathered during its 30 years organizing courses.

☐ Sign me up for Energize Weekly

How did you hear about this event? (direct e-mail, colleague, speaker(s), etc.)

Print Name

Job Title

Company

What name do you prefer on your name badge?

Address

City

State/Province

Zip/Postal Code

Country

Phone

Email

List any dietary or accessibility needs here

### CREDIT CARD INFORMATION

Name on Card

Billing Address

Account Number

Billing City

Billing State

Exp. Date

Security Code (last 3 digits on the back of Visa and MC or 4 digits on front of AmEx)

Billing Zip Code/Postal Code

**OR** Enclosed is a check for \$ \_\_\_\_\_ to cover \_\_\_\_\_ registrations.

### Substitutions & Cancellations

Your registration may be transferred to a member of your organization up to 24 hours in advance of the event. Cancellations must be received on or before March 2, 2018 in order to be refunded and will be subject to a US \$195.00 processing fee per registrant. No refunds will be made after this date. Cancellations received after this date will create a credit of the tuition (less processing fee) good toward any other EUCI event. This credit will be good for six months from the cancellation date. In the event of non-attendance, all registration fees will be forfeited. In case of course cancellation, EUCI's liability is limited to refund of the event registration fee only. For more information regarding administrative policies, such as complaints and refunds, please contact our offices at 303-770-8800. EUCI reserves the right to alter this program without prior notice.



(b) (6)

**From:** Laxmi Mrig <lmrig@euci.com>  
**Sent:** Thursday, March 08, 2018 11:38 AM  
**To:** (b) (6)  
**Subject:** Upcoming Physical & Cyber Security for Utilities Conference, April in Denver  
**Attachments:** 0418-energy-security.pdf

Hi (b) (6),

As a past attendee of the Substation Physical Security for Utilities Conference, I hope you don't mind my sending this email regarding our upcoming **Physical and Cyber Security for Utilities Conference** scheduled for **April 3-4, 2018 in Denver, CO** that I thought would be of interest either to yourself or your colleagues.

A link to the event website is: [https://www.euci.com/event\\_post/0418-energy-security/?x=29273v1Lx0101&rf=Laxmi](https://www.euci.com/event_post/0418-energy-security/?x=29273v1Lx0101&rf=Laxmi)

#### Brief Overview:

This conference will provide a comprehensive look at physical and cyber security challenges and solutions for utility systems. Attendees will gain valuable insights into the science and practical steps to at least double the assumed life expectancy of their underground (UG) cable systems.

#### Some Key Takeaways Include

- Reduce risk by securing critical infrastructure against human, physical, and cyber threats
- Examine costs and benefits of security investments
- Identify mitigation efforts that will ensure rapid recovery of plant operations in the case of security breaches
- Recognize where cyber security and physical security overlap
- Set benchmarks for intrusion detection, perimeter patrol, lighting
- Effectively upgrade security protocols when responsibilities are transferred from one department to another
- Bring older facilities up to current standards
- Explain the role power production and transmission facilities as part of the country's critical infrastructure
- Establish rapid response and recovery protocols in the case of a cyber security breach
- Define current threats to plant security based on recent incidents
- Discuss the intersection between plant safety and security
- Prepare for threats and resolve conflicts

#### Some of the expert speakers include:

- Justin Allar, Security Systems Supervisor, Platte River Power Authority
- Fred Bonewell, Chief Safety and Security Officer, CPS Energy
- Mark Bullock, Director of Security, Commonwealth Edison
- Michelle Draxton, Manager of Generation Security, Exelon Corporate and Information Security Services

- Shawn Graff, Regional Director, Region VIII, Office of Infrastructure Protection, Department of Homeland Security
- Tim Kacena, Physical Security Specialist – Investigator, Nebraska Public Power District
- Jason Maldonado, Security, Emergency Management & Safety Management, Platte River Power Authority
- Mike Reterstorf, IT Manager in NERC Compliance Office, DTE Energy
- Justin Thibault, Senior Technical Leader, EPRI

I have attached the event brochure for the above which includes a detailed agenda. Registration/hotel information can be found on the last page.

I appreciate your forwarding along to anyone who would have an interest.

Not the right event? EUCI offers hundreds of events throughout the year check [www.euci.com/events/?x=29282v1Lx0101](http://www.euci.com/events/?x=29282v1Lx0101) for our other offerings.

If you have any questions regarding the program, if you would like to register over the phone, or need the early bird rate extended, please feel free to contact me at **720-988-1211** or via email [lmrig@euci.com](mailto:lmrig@euci.com).

We hope you will be able to attend.  
Thank you for your time,

Laxmi

Laxmi Mrig  
Principal



720-988-1211 | [lmrig@euci.com](mailto:lmrig@euci.com)

For a list of upcoming events, please visit [www.euci.com](http://www.euci.com)

**Follow Us**



---

This information contained in this email and any attachments may contain confidential and/or privileged material and is the sole property of EUCI. It is intended solely for the person(s) to which it is addressed. Any review, retransmission, dissemination, or taking of any action in reliance upon this information by persons or entities other than the intended recipient(s) is prohibited. If you received this in error, please contact the sender and delete the material from any computer.



# PHYSICAL AND CYBER SECURITY FOR UTILITIES: *Protecting Generation and Transmission Facilities*

April 3-4, 2018

Courtyard by Marriott Denver Cherry Creek  
Denver, CO

## POST-CONFERENCE WORKSHOP

### **CIP-014 Compliance: Protecting the Power Grid from Physical Attack**

WEDNESDAY, APRIL 4, 2018

“

*“I am usually reluctant to attend a 1 and a half day conference, but the information provided was excellent. Totally worth my time.”*

Manager of Safety & Security, East Kentucky  
Power Cooperative



TAG US #EUCIEvents  
FOLLOW US @EUCIEvents



EUCI is authorized by  
IACET to offer 1.0 CEUs for  
the conference and 0.4  
CEUs for the workshop.

# OVERVIEW

Power companies today face unprecedented challenges when it comes to both physical and cyber security. Given the immense amount of power generated and critical role power generation and transmission facilities play in the nation's infrastructure, the cost of a security breach goes beyond mere financial damage – it can affect the safety of an entire region. For this reason alone, it is imperative for utilities and plant managers to initiate effective security protocols within their operating budgets.

Cyber security attacks on infrastructure targets are happening with increased sophistication and frequency. Each power generation site has a complicated collection of controls that may include both legacy systems and smart assets. Each system presents challenges that range from patching to the introduction of an entire array of not-well-understood vulnerabilities. Many plants are old, and upgrading them is more than a simple matter of adding new technologies. Old systems may need to be replaced or upgraded as well. When new technologies are built on top of legacy systems, new risks may emerge as different systems interact. Companies are developing multi-pronged approaches to cyber security such as threat hunting, a proactive measure to protect their systems.

Physical and Cyber Security for Utilities gives plant managers, plant operators, heads of physical, cyber and corporate security a full understanding of what is at stake when it comes to securing their plant and how they can ensure the safety and security of their operations. The symposium will cover the role of power generation plants and T&D facilities as part of the nation's critical infrastructure. Attendees will learn to recognize the external drivers and regulatory requirements for plant physical security. They will learn to organize their plants and substations for cyber and physical security as well as safety. Attention will be paid to how to assess and upgrade a facility's current security organization. Experts will review how to apply cyber security guidelines and advanced technologies for power generation and transmission security programs. Finally, there will be a "utilities Q&A" so attendees can ask their own questions of how utilities are handling their security protocols.

# LEARNING OUTCOMES

- Reduce risk by securing critical infrastructure against human, physical, and cyber threats
- Examine costs and benefits of security investments
- Identify mitigation efforts that will ensure rapid recovery of plant operations in the case of security breaches
- Recognize where cyber security and physical security overlap
- Set benchmarks for intrusion detection, perimeter patrol, lighting
- Effectively upgrade security protocols when responsibilities are transferred from one department to another
- Bring older facilities up to current standards
- Explain the role power production and transmission facilities as part of the country's critical infrastructure
- Establish rapid response and recovery protocols in the case of a cyber security breach
- Define current threats to plant security based on recent incidents
- Discuss the intersection between plant safety and security
- Prepare for threats and resolve conflicts

# WHO SHOULD ATTEND

Directors of Operations, Heads of Security, Cyber and Corporate Security Managers from Power Generation and Transmission Facilities, Security Companies, Software Companies, Law Firms, and Engineering Firms.

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)



# AGENDA

TUESDAY, APRIL 3, 2018

**8:00 – 8:30 am**

## **Registration and Continental Breakfast**

**8:30 – 9:30 am**

## **Power Production and Transmission as Critical Infrastructure**

More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to various industries, households and businesses. The energy infrastructure contains more than 6,413 power plants which includes 3,273 traditional electric utilities and 1,738 nonutility power producers with approximately 1,075 gigawatts of installed generation. Electricity generated at power plants is transmitted over 203,930 miles of high-voltage transmission lines. The electricity infrastructure is highly automated and controlled by utilities and regional grid operators nationwide; therefore, it is imperative for owners and operators to collaborate and coordinate to ensure the security and resilience of the grid due to its' complex operating structure and it's critical and essential function across virtually all critical infrastructure sectors. This presentation will discuss:

- Assessing security risks and threats to power plants
- Securing critical infrastructure from all hazards
- Enhancing critical infrastructure resilience
- Sharing information to enable risk-informed decision making
- Adopting, learning, and adaptation in the face of changing conditions

***Shawn Graff, Regional Director, Region VIII, Office of Infrastructure Protection, Department of Homeland Security***

**9:30 – 10:30 am**

## **A Forward Thinking Approach for Developing a Physical and Cyber Security Plan for Low Impact Assets**

Developing a physical and cyber security plan to implement at Low Impact generation sites is an exercise in planning for current state as well as future proofing for changes in physical infrastructure and changing requirements. Existing Low Impact assets have a broad range of capabilities, risks, age in equipment, and operational considerations even within the same entity. Developing an approach to ensure consistency, operational flexibility, and reduce overall cyber and physical risk is a challenge. This presentation will look at using a risk based approach to developing a program to implement Physical and cyber security plans to support existing and future low impact sites.

- Developing a program that supports existing aging low impact assets and future development
- Using a risk assessment to identify controls based on individual sites
- Developing programs that separate controls for physical and cyber security plans
- Implementing controls that can be implemented across high, medium, and low impact assets but scaled to impact level
- Presenting an example using DTE Energy's medium and low impact generations sites implementation program

***Mike Reterstorf, IT Manager in NERC Compliance Office, DTE Energy***

**10:30 – 11:00 am**

## **Networking Break**

**11:00 – 11:45 am**

## **Assessing Plant Physical Security: The Newcomer's Perspective**

- Assessing an established organization for security risk factors
- Fortification of existing intrusion detection
- Intrusion detection and monitoring
- Policies and programs
- Integrating company culture with new initiatives

***Jason Maldonado, Security, Emergency Management & Safety Management, Platte River Power Authority***

***Justin Allar, Security Systems Supervisor, Platte River Power Authority***

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)



# AGENDA

TUESDAY, APRIL 3, 2018 (CONTINUED)

## 11:45 am – 12:30 pm **Intersections: The Overlap Between Safety and Security**

- Regulatory compliance and what drives it
  - NERC/FERC requirements
  - OSHA requirements
- Duty to protect employees
  - Threats of workplace violence
- Emergency management and incident response
  - Roles of safety professionals vs. security professionals

**Jason Maldonado, Security, Emergency Management & Safety Management, Platte River Power Authority**

**Justin Allar, Security Systems Supervisor, Platte River Power Authority**

## 12:30 – 1:30 pm **Group Luncheon**

## 1:30 – 2:30 pm **Collaborative R&D in Securing Power Generation**

The increasing sophistication and frequency of cyber security attacks on infrastructure targets is another example of the unprecedented challenges to power generators today. In response, regulations around the globe are requiring an active cyber security strategy for all power generation, significantly more complex than traditional controls network segregation (i.e. "air-gapping").

The core cyber security challenge is that each power generation site is deploying more digital Industrial Control System (ICS) assets from a variety of vendors as a result of obsolescence, and to take advantage of performance gains. These various digital systems and components are more highly integrated than ever before resulting in a larger cyber security attack surface. The rapidly evolving threat landscape and sophisticated ICSs present both a technical and organizational challenge for developing, implementing, and maintaining a successful cyber security program. On top of the numerous technical challenges, cultural and programmatic gaps need to be addressed in a consistent and coordinated approach.

EPRI's Generation Sector has been leveraging industry resources and R&D efforts in the Nuclear and Power Delivery programs to tailor research to power generation. Included in this presentation will be the following:

- NIST Level 4, decentralized hardware-based Remote Access Solution that could streamline management of interactive remote access
- Utilizing proven enterprise architecture techniques to facilitate IT/OT integration in Power Generation
- Research into real-time detection capabilities to better automate threat detection
- A new technical assessment optimization methodology that protects against emerging threats and the added costs of changing regulation

Most importantly, EPRI has been developing a community of industry peers dedicated to securing power generation. This presentation will describe how others in the industry can leverage this resource.

**Justin Thibault, Senior Technical Leader, EPRI**

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)



# AGENDA

TUESDAY, APRIL 3, 2018 (CONTINUED)

**2:30 – 3:00 pm**

## **Networking Break**

**3:00 – 4:00 pm**

## **Confronting Active Shooters in a Utility Setting: Preparing for Threats**

The presentation will provide methods on how to train and drill for an active shooter in and out of the workplace. Some topics that will be covered will include, recognizing signs of an active shooter before an incident happens, how to act on the signs, how to increase your chances for survival in a moment of crisis, and providing tips on how to conduct active shooter drills.

- Active shooter/killer trends
- Active killer response and developing the survival mentality
- Tips on how to perform an active shooter drill

***Tim Kacena, Physical Security Specialist – Investigator, Nebraska Public Power District***

**4:00 – 5:00 pm**

## **Conflict Resolution Training for Utilities**

This session covers conflict resolution in the workplace, primarily teaching how to deal with difficult customers in stressful situations to avoid escalation. Actual footage of events will be used as well as group discussion.

- What training are we giving co-workers to de-escalate dangerous situations?
- Identify stressful situations that employees could encounter
- Determine an appropriate time to contact law enforcement

***Tim Kacena, Physical Security Specialist – Investigator, Nebraska Public Power District***

**5:00 pm**

## **End of Day One**

WEDNESDAY, APRIL 4, 2018

**8:00 – 8:30 am**

## **Continental Breakfast**

**8:30 – 9:30 am**

## **Threat Hunting for Cyber Risks**

Implementing a complex layered security approach with multiple reporting tools alerting on infections and signatures is no longer an acceptable security approach. Everyone likes to use the words “proactive security” but what exactly does that mean? This talk will go over a proactive security approach known as threat hunting, how it varies from current cybersecurity practices, what it’s going to take to implement, and how threat hunting can improve your cybersecurity landscape.

- What is Threat Hunting
- Current Cyber Practices (Reactive) vs Threat Hunting (Proactive)
- Review use cases where this has occurred, where in certain environments a “hack proof” defense can be created
- What’s it going to take
  - o Analyst functions
  - o Network Analysis
  - o Host Analysis
- Is this possible in an ICS Environment?

***Fred Bonewell, Chief Safety and Security Officer, CPS Energy***

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)





# AGENDA

WEDNESDAY, APRIL 4, 2018 (CONTINUED)

**9:30 – 10:30 am**

## **Implementing Substation Physical Security Risks and Controls**

For years security departments have worked with law enforcement in response to copper thefts from substations. The Metcalf substation ballistic attack in 2013 along with other criminal and terrorist threats have brought to light substation risks and made it clear that robust physical security of substations is needed to protect against disruption of operations. At critical sites, controls must deter, detect, delay, communicate and allow for a prompt response. A defense in depth strategy is required to reduce risks and vulnerabilities associated with unauthorized access to personnel, equipment, systems and materials. This session will cover processes needed to effectively mitigate substation physical security risks:

- To effectively mitigate substation physical security risks:
- Working closely with operational functions to understand and document substations criticality to operations, and tier accordingly
- Identifying and delineating control requirements for each tier considering risks of unauthorized access to substations and operational impacts
- Assessing capital expenditures and subsequent maintenance costs
- Conducting periodic site security assessments to identify new vulnerabilities and tracking any issues that are identified until they are addressed
- Developing processes to continuously assess criminal and terrorist risks that may threaten substations and creating new risks mitigation strategies

**Mark Bullock, Director of Security, Commonwealth Edison**

**10:30 – 11:00 am**

## **Networking Break**

**11:00 am – 12:00 pm**

## **Mitigate Risk to Generation Assets through an Assessment Program**

Strategic enhancements to the existing Physical Security Assessment process can result in improved analysis of physical security application and risk management at generation facilities. This session covers an approach that was developed to deploy protection measures through corporate governance to minimize security risk.

- To effectively mitigate physical security risks
- collaborate with Business Unit and operational functions to understand and document criticality to operations, and tier accordingly
- Identify and standardize minimum Security Protection Standards as countermeasures elements of the Security Assessment process
- Implement a prototype system to facilitate proof of concept in Security Assessment performance
- Perform periodic Site Security Assessments based on tier to validate protection measures
- Determine acceptable risk tolerance level
- Develop and Implement Program Governance for a uniform methodology of performing Security Assessments to mitigate risk

**Michelle Draxton, Manager of Generation Security, Exelon Corporate and Information Security Services**

**12:00 pm**

## **Symposium Concludes**

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)

## POST-SYMPOSIUM WORKSHOP

# CIP-014 Compliance: Protecting the Power Grid from Physical Attack

WEDNESDAY, APRIL 4, 2018

**12:30 – 1:00 pm**      **Workshop Registration****1:00 – 4:00 pm**      **Workshop Timing**

## OVERVIEW

Securing the North American power grid is a top priority for both regulators and utilities. While the industry remains focused on grid resilience, physical security threats remain that could affect generation, transmission, and distribution operations. A coordinated and simultaneous attack on multiple high voltage transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts. Such an event would have serious economic and social consequences. While adversaries are becoming more informed and highly capable, we will discuss recent physical security events, NERC CIP-014 compliance, and strategies to reduce overall threats and vulnerabilities.

## LEARNING OUTCOMES

- Find out what industry is doing today to better protect critical electric infrastructure and identify emerging threats facing substations, generating plants, and energy control centers
- Implement the NERC CIP-014 standard, mitigation strategies, and effective compliance
- Recognize how utilities can incorporate deter, detect, and delay into their physical security program to meet compliance and become a “hard target”

## WORKSHOP AGENDA

**1:00 – 2:30 pm****Physical Threats to the Grid**

Participants will learn about recent physical attacks against energy infrastructure, including an in-depth analysis of the 2013 California substation shooting, which was the catalyst for the NERC CIP-014 standard. Also discussed will be how to conduct a proper threat and vulnerability assessment that will feed into a comprehensive physical security response plan.

We will Discuss:

- Physical Attack Scenarios
- The April 16, 2013 Metcalf Substation Shooting
- The Insider Threat
- Emerging Threats Including Drones and Civil Unrest

**2:30 – 3:00 pm****Coffee Break**REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)

# WORKSHOP AGENDA

**3:00 – 5:00 pm****Deter, Detect, Delay, Assess, Communicate, and Respond Under NERC CIP-014**

Learn how to incorporate the information from a threat and vulnerability assessment and apply it to a mitigation strategy and future road map. Participants will learn specifics about the NERC-014 standard, how to achieve compliance, and ensuring you have properly protected the “crown jewels”.

We will Discuss:

- Physical Security Technologies Being Used in Industry
- How to Create a Robust Physical Security Plan
- CIP-014 R4, R5, and R6 Insights
- Engaging the Regulator and Information Sharing

**5:00 pm****Workshop Concludes**

# WORKSHOP INSTRUCTOR

**Brian Harrell****CPP, Vice President of Security, AlertEnterprise**

Brian Harrell, CPP, is the Vice President of Security at AlertEnterprise, a technology and advisory firm that provides critical infrastructure owners with consultation on physical and cybersecurity protections. He is the former Operations Director of the Electricity ISAC and Director of Critical Infrastructure Protection Programs at the North American Electric Reliability Corporation (NERC) where he was charged with helping protect North America's electric grid from physical and cyber-attack. Brian was a Standard Drafting Team (SDT) member for the NERC physical security standard, CIP-014. Brian has spent time during his career in the US Marine Corps, US Department of Homeland Security, and various private sector agencies with the goal of protecting the United States from security threats. Brian is also a Senior Fellow at The George Washington University Center for Cyber & Homeland Security (CCHS) where he provides insight and analysis on homeland security, counterterrorism, and cybersecurity issues.

**REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)**

# REQUIREMENTS FOR SUCCESSFUL COMPLETION

Participants must sign in/out each day and be in attendance for the entirety of the course to be eligible for continuing education credit.

## INSTRUCTIONAL METHODS

Powerpoint presentations and case studies will be used throughout this conference

## IACET CREDITS



EUCI has been accredited as an Authorized Provider by the International Association for Continuing Education and Training (IACET). In obtaining this accreditation, EUCI has demonstrated that it complies with the ANSI/IACET Standard which is recognized internationally as a standard of good practice. As a result of their Authorized Provider status, EUCI is authorized to offer IACET CEUs for its programs that qualify under the ANSI/IACET Standard.

**EUCI is authorized by IACET to offer 1.0 CEUs for the conference and 0.4 CEUs for the workshop.**

## EVENT LOCATION

A room block has been reserved at the Courtyard by Marriott Denver Cherry Creek, 1475 S Colorado Blvd, Denver, CO 80222, for the nights of April 2-3, 2018. Room rates are \$139 plus applicable tax. Call **1-303-757-8797** or [click here](#) for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is March 12, 2018 but as there are a limited number of rooms available at this rate, the room block may close sooner. ***Please make your reservations early.***

## REGISTER 3, SEND THE 4TH FREE

Any organization wishing to send multiple attendees to this event may send 1 FREE for every 3 delegates registered. Please note that all registrations must be made at the same time to qualify.

REGISTER TODAY! CALL 303-770-8800 OR VISIT [WWW.EUCI.COM](http://WWW.EUCI.COM)



# REGISTRATION INFORMATION

## Mail Directly To:

EUCI  
4601 DTC Blvd., Ste. 800  
Denver, CO 80237  
OR, scan and email to: [conferences@euci.com](mailto:conferences@euci.com)

**WWW.EUCI.COM**  
**p: 303-770-8800**  
**f: 303-741-0849**

## PLEASE REGISTER

☐ **BOTH PHYSICAL AND CYBER SECURITY FOR UTILITIES AND POST- CONFERENCE WORKSHOP**

APRIL 3-4, 2018: US \$1795

Early bird on or before March 16, 2018: US \$1595

☐ **PHYSICAL AND CYBER SECURITY FOR UTILITIES ONLY**

APRIL 3-4, 2018: US \$1395

Early bird on or before March 16, 2018: US \$1195

☐ **POST-CONFERENCE WORKSHOP ONLY**

APRIL 4, 2018: US \$595

Early bird on or before March 16, 2018: US \$495

☐ **I'M SORRY I CANNOT ATTEND, BUT PLEASE EMAIL ME A LINK TO THE CONFERENCE PROCEEDINGS FOR US \$395**

Redacted Pursuant to FOIA Exemption 6

## EVENT LOCATION

A room block has been reserved at the Courtyard by Marriott Denver Cherry Creek, 1475 S Colorado Blvd, Denver, CO 80222, for the nights of April 2-3, 2018. Room rates are \$139 plus applicable tax. Call **1-303-757-8797** or [click here](#) for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is March 12, 2018 but as there are a limited number of rooms available at this rate, the room block may close sooner. **Please make your reservations early.**

## ENERGIZE WEEKLY

EUCI's Energize Weekly e-mail newsletter compiles and reports on the latest news and trends in the energy industry. Newsletter recipients also receive a different, complimentary course presentation every week on a relevant industry topic. The presentations are selected from a massive library of more than 1,000 current presentations that EUCI has gathered during its 30 years organizing courses.

☐ **Sign me up for Energize Weekly**

How did you hear about this event? (direct e-mail, colleague, speaker(s), etc.)

Print Name

Job Title

Company

What name do you prefer on your name badge?

Address

City

State/Province

Zip/Postal Code

Country

Phone

Email

List any dietary or accessibility needs here

### CREDIT CARD INFORMATION

Name on Card

Billing Address

Account Number

Billing City

Billing State

Exp. Date

Security Code (last 3 digits on the back of Visa and MC or 4 digits on front of AmEx)

Billing Zip Code/Postal Code

**OR** Enclosed is a check for \$ \_\_\_\_\_ to cover \_\_\_\_\_ registrations.

### Substitutions & Cancellations

Your registration may be transferred to a member of your organization up to 24 hours in advance of the event. Cancellations must be received on or before March 2, 2018 in order to be refunded and will be subject to a US \$195.00 processing fee per registrant. No refunds will be made after this date. Cancellations received after this date will create a credit of the tuition (less processing fee) good toward any other EUCI event. This credit will be good for six months from the cancellation date. In the event of non-attendance, all registration fees will be forfeited. In case of course cancellation, EUCI's liability is limited to refund of the event registration fee only. For more information regarding administrative policies, such as complaints and refunds, please contact our offices at 303-770-8800. EUCI reserves the right to alter this program without prior notice.





From: [Comcast](#)  
To: (b) (6)  
Date: Monday, April 02, 2018 4:38:00 PM  
Attachments: [R45135.pdf](#)

---

<https://fas.org/sgp/crs/homsec/R45135.pdf>



# NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?

**Paul W. Parfomak**

Specialist in Energy and Infrastructure Policy

March 19, 2018

**Congressional Research Service**

7-5700

[www.crs.gov](http://www.crs.gov)

R45135

## Summary

A 2013 rifle attack on a critical electric power substation in Metcalf, CA, marked a turning point for the U.S. electric power sector. The attack prompted utilities across the country to reevaluate and restructure their physical security programs. It also set in motion proceedings in Congress and at the Federal Energy Regulatory Commission (FERC) which resulted in a new mandatory *Physical Security Reliability Standard* (CIP-014) for bulk power asset owners promulgated by the North American Electric Reliability Corporation (NERC) in 2015. In the three years since FERC approved this new standard, security risks to the power grid have become an even greater concern in the electric utility industry. Reflecting these ongoing security concerns, legislative proposals in the 115<sup>th</sup> Congress include provisions directed at power grid physical security. Congress also continues its oversight of grid security and implementation of NERC's security standards.

Three entities play key roles in standards oversight and support of implementation for bulk power physical security. NERC and FERC oversee implementation of the CIP-014 standards, while the Department of Energy plays a supporting role in helping bulk power asset owners to protect their critical infrastructure. The detailed findings of NERC's compliance activities are not publicly disclosed due to their confidential nature. However, NERC has stated that the utility industry is making progress towards effective implementation of the CIP-014 standard and NERC has been "encouraged" by grid security measures put in place so far. NERC compliance audits as of February 2018 have uncovered no major failures to date.

In addition to compliance with NERC's standards, there have been other observable changes within the electricity sector reflecting greater emphasis on bulk power physical security. These changes include realignment in corporate structure to support physical security, incorporating physical security in transmission planning, new security products and services, utility capital investment in physical security, and utility participation in voluntary security programs. While public information about such changes is limited, it suggests they may be significant and widespread.

Although the electric power sector seems to be moving in the overall direction of greater physical security for critical assets, many measures have yet to be implemented and the process of corporate realignment around physical security is still underway. NERC's CIP-014 standards have been promulgated recently, and bulk power asset owners have largely begun enhancing physical security under the standard over the last two years. Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector's own assessments of risk. Bulk power security remains a work in progress.

Congress continues to be concerned about the current state of electric grid physical security. Among many specific issues of potential interest, Congress may focus on several with policy significance: security implementation oversight, cost recovery, hardening vs. resilience, and the quality of threat information. As CIP-014 implementation and other physical security initiatives proceed, Congress also may seek to maintain its focus on the power sector's overall progress, not only on short term compliance with NERC's security standards, but also on structural changes supporting physical security as a priority far into the future.

## Contents

Introduction .....	1
Power Grid Threat Environment .....	2
NERC's Physical Security Standards .....	3
Physical Security Standard Requirements.....	4
Federal Oversight and Support.....	4
NERC's Implementation Oversight .....	5
Electricity Information Sharing and Analysis Center .....	6
FERC Oversight.....	7
DOE Initiatives.....	8
Observed Changes in Bulk Power Physical Security .....	9
Corporate Structure Supporting Physical Security.....	9
Physical Security in Long-Term Transmission Planning .....	11
New Security Products and Services.....	12
Capital Investment in Physical Security.....	13
Utility Participation in Voluntary Security Programs.....	14
NERC Grid Security Exercises.....	14
DHS Critical Infrastructure Surveys .....	15
Legislative Proposals in the 115 <sup>th</sup> Congress .....	15
Policy Issues for Congress.....	16
Oversight of Physical Security Implementation.....	17
Financial Requirements and Cost Recovery .....	18
Hardening vs. Resilience.....	18
Threat Information .....	19
Conclusion.....	20

## Contacts

Author Contact Information .....	21
----------------------------------	----

## Introduction

Securing the electric power grid is among the highest priorities for critical infrastructure protection in the United States. In the past, power grid facilities have had varying degrees of access control and surveillance depending upon the facility type and location. These measures were largely focused on public safety (reflecting liability concerns) and preventing vandalism and theft. More recently, federal agencies, Congress, and the utility industry have focused greater attention on the vulnerability of the power grid, especially the high voltage transmission (bulk power) system, to terrorist attacks which could cause widespread, extended blackouts.

Until 2013, the emphasis of analysts and policymakers was on power grid cybersecurity—protecting the computer controls and communication systems used to operate the grid. However, a 2013 rifle attack on an electric transmission substation in Metcalf, CA, shifted more attention to the physical security of power grid critical assets. In response to the Metcalf attack, as well as other grid incidents and findings from utility security exercises, Congress passed new legislation to strengthen power grid physical security and to facilitate recovery in the event of a successful attack.<sup>1</sup> Congress also sought stronger physical security standards from the Federal Energy Regulatory Commission (FERC) under the commission’s existing statutory authority to regulate the reliability of the bulk power system. FERC, in turn, ordered the North American Electric Reliability Corporation (NERC)—the not-for-profit organization responsible for ensuring grid reliability—to promulgate new requirements for the physical security of bulk power critical infrastructure.<sup>2</sup> After consultation within the utility industry, NERC proposed new physical security standards in May 2014. FERC approved them, with minor changes, the following November.<sup>3</sup>

Since 2014, security risks to the power grid have become an even greater concern in the electric utility industry. Addressing them has remained a concern of Congress.<sup>4</sup> An emphasis on physical risk to the power grid was underscored in September 2016 by another successful rifle attack on a transformer substation—in Utah. Reflecting ongoing security concerns, legislative proposals in the 115<sup>th</sup> Congress include provisions directed at power grid physical security. Congress also continues its oversight of FERC’s grid security activities and the implementation of NERC’s physical security standards.

This report examines changes to the physical security of the electric power grid since the promulgation of NERC’s physical security standards. The report discusses the current risk environment for the bulk power system. It summarizes the key requirements of NERC’s security standards, including its applicability to specific assets, implementation deadlines, and oversight. The report reviews observable changes in the utility sector related to physical security. It concludes with an overview of proposed legislation and a discussion of policy issues for Congress.

---

<sup>1</sup> The Fixing America’s Surface Transportation (FAST) Act (P.L. 114-94), which became law on December 4, 2015, contains provisions to protect or restore the reliability of critical electric infrastructure or defense of critical electric infrastructure during a grid security emergency (§1104).

<sup>2</sup> Among other functions, NERC develops and enforces reliability standards, monitors the grid, and trains industry personnel. In the United States, NERC is subject to Federal Energy Regulatory Commission oversight.

<sup>3</sup> For more historical background and details regarding the development of NERC’s standards, see CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak.

<sup>4</sup> See for example: Senator Ron Johnson, Chairman, Opening statement before the Senate Committee on Homeland Security and Governmental Affairs hearing on “Threats to the Homeland,” September 27, 2017.



This report focuses primarily on physical security efforts to prevent successful physical attacks on the bulk power system. For analysis of issues specifically related to power grid cyberattacks and cybersecurity, see CRS Report R43989, *Cybersecurity Issues for the Bulk Power System*, by Richard J. Campbell. This report also does not address issues related to security incident recovery or restoration, except in the context of preventive physical security.

## Power Grid Threat Environment

Grid security analysts and policymakers have long been aware of physical risks to bulk power critical infrastructure, especially to high voltage (HV) transformer stations and substations, which serve as key nodes within the electric transmission system.<sup>5</sup> The 2013 Metcalf attack, in which an unknown perpetrator firing a .30 caliber rifle disabled a critical 500 kilovolt (kV) transformer substation, demonstrated that such facilities face real and potentially sophisticated threats.<sup>6</sup> The September 2016 rifle attack on a 69 kV transformer substation in Utah—which reportedly left 13,000 rural customers without power for up to eight hours—showed that similar incidents could occur almost anywhere on the grid.<sup>7</sup> A successful cyberattack on Ukraine’s power grid in 2015, which was reportedly attributed to Russian hackers, showed that foreign entities could view power grids as attractive targets.<sup>8</sup> A 2017 report from the National Academy of Sciences concludes: “While to date there have been only minor attacks on the power system in the United States, large-scale physical destruction of key parts of the power system by terrorists is a real danger. Some physical attacks could cause disruption in system operations that last for weeks or months.”<sup>9</sup>

The persistent threat environment has been changing the perception of physical threats among power grid owners and operators. For example, surveys of electric utility employees show that their physical (and cyber) security concerns are growing.<sup>10</sup> Exelon Corporation, one of the nation’s largest utility holding companies, stated in its 2016 annual report:

Threat sources continue to seek to exploit potential vulnerabilities in the electric...utility industry associated with protection of sensitive and confidential information, grid infrastructure and other energy infrastructures, and such attacks and disruptions, both physical and cyber, are becoming increasingly sophisticated and dynamic....The risk of these system-related events and security breaches occurring continues to intensify....<sup>11</sup>

Xcel Energy, another major utility owner, likewise states in its 2016 annual report:

---

<sup>5</sup> See, for example: National Research Council, *Terrorism and the Electric Power Delivery System*, 2012 and Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, June 1990.

<sup>6</sup> RTO Insider, “Substation Saboteurs ‘No Amateurs,’” April 2, 2014, <http://www.rtoinsider.com/pjm-grid2020-1113-03/>.

<sup>7</sup> Pat Reavy, “Power Company Offers Rare \$50K Reward for Information on Vandalism,” *Deseret News*, September 29, 2016. A substation rated at 69 kilovolts is not considered a “high voltage” transmission asset, although it may still serve large numbers of customers.

<sup>8</sup> Jim Finkle, “U.S. Firm Blames Russian ‘Sandworm’ Hackers for Ukraine Outage,” *Reuters*, January 7, 2016. The attack reportedly cut power to 80,000 customers for about six hours.

<sup>9</sup> National Academy of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation’s Electricity System*, 2017, p. 65, <https://doi.org/10.17226/24836>.

<sup>10</sup> Utility DIVE, *2017 State of the Electric Utility Survey*, April 10, 2017, [https://s3.amazonaws.com/dive\\_assets/rlpsys/SEU\\_2017.pdf](https://s3.amazonaws.com/dive_assets/rlpsys/SEU_2017.pdf).

<sup>11</sup> Exelon Corporation, *Annual Report Pursuant to Section 13 or 15(d) of the Securities and Exchange Act of 1934 for the Fiscal Year Ended December 31, 2016*, Form 10-K, February 13, 2017, p. 63.

Our generation plants, fuel storage facilities, transmission and distribution facilities and information systems may be targets of terrorist activities... The potential for terrorism has subjected our operations to increased risks and could have a material effect on our business.<sup>12</sup>

Accordingly, electricity sector-wide security exercises conducted by NERC have simulated attacks on power grid critical assets combining both cyber and physical dimensions.<sup>13</sup> These exercises are further discussed later in this report.

## NERC's Physical Security Standards

On March 7, 2014, FERC ordered NERC to submit proposed reliability standards requiring transmission owners meeting certain criteria “to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation” of the power grid.<sup>14</sup> In its order FERC stated that physical security standards were necessary because “the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks.”<sup>15</sup> According to the FERC order, the new reliability standards were to require transmission owners or operators to perform a risk assessment of their systems to identify “critical facilities,” evaluate the potential threats and vulnerabilities to those identified facilities, and develop and implement a security plan designed to protect against physical attacks on those identified critical facilities.<sup>16</sup> The order required that each of these steps be verified by NERC or another third party qualified to review them.

On May 23, 2014, NERC filed with FERC its proposal for mandatory physical security standards.<sup>17</sup> On November 20, 2014, FERC approved the proposed standard, with minor changes, as NERC's new *Physical Security Reliability Standard* (CIP-014-1).<sup>18</sup> Following publication in the *Federal Register*, FERC's order approving the standard became effective on January 26, 2015.<sup>19</sup> FERC approved a revised version of the standard (CIP-014-2) on July 14, 2015.<sup>20</sup> Required compliance for the standard began on October 1, 2015 with completion of the final parts required by November 24, 2016 for all applicable entities.

<sup>12</sup> Excel Energy, Inc. *Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2016*, Form 10-K, p. 44.

<sup>13</sup> North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014 and *Grid Security Exercise, GridEx III Report*, March 2016; Scott Heffentrager, PJM Interconnection, “GridEx IV Summary,” slide presentation, November 27, 2017, <http://www.pjm.com/-/media/committees-groups/committees/mc/20171127-webinar/20171127-item-04-2017-gridex-iv-summary.ashx>.

<sup>14</sup> Federal Energy Regulatory Commission (hereinafter, FERC), *Reliability Standards for Physical Security Measures*, Order Directing Filing of Standards, Docket No. RD14-6-000, March 7, 2014, p.1, <http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf>.

<sup>15</sup> FERC, March 7, 2014, p. 2.

<sup>16</sup> FERC, March 7, 2014, pp. 3-4.

<sup>17</sup> NERC, Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-014-1, May 23, 2014, <http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Physical%20Security%20CIP-014-1.pdf>.

<sup>18</sup> FERC, “Physical Security Reliability Standard,” Docket No. RM14-15-000, Order No. 802, November 20, 2014.

<sup>19</sup> NERC, “Physical Security Reliability Standard Implementation,” January 16, 2015, [http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20\(Agenda%20Excerpt\).pdf](http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20(Agenda%20Excerpt).pdf).

<sup>20</sup> FERC, letter order to the North American Electric Reliability Corporation, Docket No. RD-15-4-000, July 14, 2015, [http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Letter\\_Order\\_CIP-014\\_20150714\\_RD15-4.pdf](http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Letter_Order_CIP-014_20150714_RD15-4.pdf).

## Physical Security Standard Requirements

The stated purpose of NERC’s physical security reliability standard is “to identify and protect transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or cascading within an interconnection.”<sup>21</sup> It applies to transmission owners with assets operating at 500 kV or higher as well as owners with substations operating between 200 kV and 499 kV if they meet certain interconnection or load-carrying criteria.<sup>22</sup> The standard, generally referred to as “CIP-014,” consists of six principal requirements (R1-R6), summarized as follows:

- R1. Risk assessments by transmission owners to identify critical transmission facilities;
- R2. Independent third party verification of risk assessments conducted under R1;
- R3. Requirement for transmission owners with critical facilities identified under R1 but not under their operational control to notify the transmission operator of these facilities;<sup>23</sup>
- R4. Mandatory threat and vulnerability assessments for critical facilities conducted by transmission owners and operators;
- R5. Development, documentation, and implementation of physical security plans to protect critical facilities; and
- R6. Independent third party review of the threat and vulnerability assessments performed under R4 and security plans developed under R5.<sup>24</sup>

The standard also lays out a process for compliance monitoring and assessment including audits, self-certifications, spot checking, violation investigations, self-reporting, and handling complaints.<sup>25</sup> The new standard is enforced by NERC or another Regional Entity under a penalty review policy for mandatory reliability standards approved by FERC subject to the Commission’s enforcement authority and oversight under the Energy Policy Act of 2005 (P.L. 109-58).<sup>26</sup> Monitoring of compliance with the standard is further discussed below.

## Federal Oversight and Support

Three entities play key roles in standards oversight and implementation support for bulk power physical security. NERC and FERC directly oversee implementation of the CIP-014 standards, while the Department of Energy (DOE) plays a supporting role in helping bulk power asset owners to protect their critical assets.

---

<sup>21</sup> NERC, *CIP-014-2 – Physical Security*, printed December 5, 2017, p. 1, available at [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical%20Security&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical%20Security&jurisdiction=United%20States). (Hereinafter CIP-014-2). This report uses the terms “critical assets” and “critical substations” to mean “critical transmission stations and transmission substations” as defined under the CIP-014 standard.

<sup>22</sup> CIP-014-2.

<sup>23</sup> A regional transmission operator (RTO) administers the transmission grid for multiple transmission owners in a specified region in accordance with FERC Order No. 2000. RTOs and independent system operators (ISOs) are defined in Section 3 of the Federal Power Act (16 U.S.C. 796).

<sup>24</sup> CIP-014-2, pp. 3-6.

<sup>25</sup> CIP-014-2, p.8.

<sup>26</sup> FERC, *Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672*, Docket Nos. AD08-6-000 and RM05-30-002, April 17, 2008.

## NERC's Implementation Oversight

As stated above, with oversight by FERC, NERC has the authority to develop, oversee, and enforce implementation of the CIP-014 physical security standard.<sup>27</sup> NERC carries out these functions together with the eight Regional Entities (e.g., Midwest Reliability Organization) with which NERC has agreements to delegate its authority to monitor and enforce reliability standards compliance.<sup>28</sup> Collectively, NERC and the Regional Entities comprise the Electric Reliability Organization (ERO) Enterprise.

In general, NERC employs a risk-based framework to monitor compliance of all its grid reliability standards on the belief that monitoring and enforcement must be “right-sized” based on considerations including risk factors and management practices related to detecting, assessing, mitigating, and reporting of noncompliance.<sup>29</sup>

As reliability risk is not the same for all registered entities, the Framework examines [bulk power system] risk of registered entities both collectively and individually, to determine the most appropriate [Compliance Monitoring and Enforcement Program] tool to use when monitoring a registered entity's compliance with NERC Reliability Standards. The Framework also promotes an examination into how registered entities operate and tailor compliance monitoring focus to areas that pose the greatest risk to [bulk power system] reliability.<sup>30</sup>

NERC's approach offers flexibility in both the frequency and type of compliance monitoring (e.g., offsite or onsite audits, spot checks, or self-certifications) applied to an entity under a particular standard based on its particular level of reliability risk.<sup>31</sup> To support its compliance approach, NERC may conduct various activities, such as publishing guidance documents, providing training, and conducting outreach, “to promote transparency and confidence” in the utility industry's implementation of a standard.<sup>32</sup>

In monitoring compliance of the CIP-014 standard, NERC's focus in 2015 and 2016 was on the standards' requirements to identify critical transmission stations and substations (Requirements R1 and R2), ensuring that this identification was “appropriate and risk-informed.”<sup>33</sup> NERC required covered entities to self-certify with respect to: risk-assessment, identifying critical assets, and third party verification. NERC also conducted voluntary outreach through on-site visits with 19 covered entities to discuss security measures and CIP-014 implementation challenges.<sup>34</sup> In

<sup>27</sup> NERC's authorities to monitor compliance with its reliability standards and impose financial penalties are found in FERC regulations at 18 C.F.R. 39.7.

<sup>28</sup> See NERC, “Key Players,” web page, March 13, 2018, <http://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>.

<sup>29</sup> NERC, *Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program*, September 5, 2014, p. iv.

<sup>30</sup> NERC, *2017 ERO Enterprise Compliance Monitoring and Enforcement Implementation Plan, Version 2.5*, May 2017, p. 3.

<sup>31</sup> NERC, May 2017, p. 3.

<sup>32</sup> NERC, “Physical Security Reliability Standard Implementation,” January 16, 2015, p. 3, [http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20\(Agenda%20Excerpt\).pdf](http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20(Agenda%20Excerpt).pdf)

<sup>33</sup> NERC, May 2017, p. 16.

<sup>34</sup> NERC, *2016 ERO Enterprise Compliance Monitoring and Enforcement Program Annual Report*, February 8, 2017, p. 18, <http://www.nerc.com/pa/comp/CE/Compliance%20Violation%20Statistics/2016%20Annual%20CMEP%20Report.pdf>.

cases where there have been discrepancies between utility-generated critical asset lists and critical assets identified by the independent third parties, NERC has required the covered entities to provide further information and explanation to address the discrepancy. NERC has also been conducting audits of entities which have identified more, or fewer, critical substations as a percentage of all their substations than is typical.<sup>35</sup> The detailed findings of NERC's compliance activities are not publically disclosed due to the confidential nature of security information. However, NERC stated that, based on observations in 2016, the utility industry was "making progress towards effective implementation of and compliance with CIP-014-2."<sup>36</sup> A NERC presentation about its voluntary and informal site visits reported "remarkable progress" on physical security among 19 asset owners visited as of February 2016.<sup>37</sup>

In 2017, NERC increased its focus on the scope of utility security plans (R5), including their timelines for implementing security measures and the utility industry's overall progress in implementing CIP-014. The ERO Enterprise has prioritized auditing the quality of covered entities' risk management plans. In the second quarter of 2017, compliance audit staff were provided with guidance and training on bulk power physical security best practices as a reference for evaluating the physical security measures implemented by the covered entities.<sup>38</sup>

The ERO Enterprise expects to complete audits of the largest entities within three years of the effective date of CIP-014. As of February 2018, NERC had conducted compliance audits of approximately 45% of the covered entities with critical transmission stations and substations as defined under CIP-014. NERC had also audited over 30% of entities that did not identify critical assets after applying the CIP-014 criteria (under R1). NERC staff expects to have audited approximately 70% of the entities with CIP-014 critical assets by the end of 2018.<sup>39</sup> According to its stated schedule, NERC would audit the remaining entities in 2019. Subsequent monitoring and enforcement will focus more heavily on implementation of measures in the grid security plans.

According to NERC, the audits completed to date have not uncovered any major compliance failures, and NERC has been "encouraged" by security measures that utilities have put in place so far.<sup>40</sup> NERC has found no serious risk violations of the CIP-014 standard. Of 19 noncompliance issues identified, 8 were found to be "minimal" or "moderate" risk, with 2 warranting a financial penalty. The remaining 11 noncompliance issues are under review.<sup>41</sup>

## Electricity Information Sharing and Analysis Center

In addition to its standards activities, NERC also supports security of the electric power sector as the operator of the Electricity Information Sharing and Analysis Center (E-ISAC). Established in

<sup>35</sup> NERC, Staff meeting with CRS analysts, Washington, DC, December 7, 2017.

<sup>36</sup> NERC, May 2017, p. 16.

<sup>37</sup> Carl Herron, NERC, "CIP-014-02 Physical Security Site Visits," slide presentation, April 14, 2016, [https://www.frc.com/Compliance/EducationalMaterials/Educational%20Materials/Workshops%20-%20Workshop%20Event%20Materials/2016-04%20-%20OP%20Spring%20Compliance%20Workshop%20\(April%202012-14\)/7.%20CIP-014-2%20Physical%20Security%20Site%20Visits.pdf](https://www.frc.com/Compliance/EducationalMaterials/Educational%20Materials/Workshops%20-%20Workshop%20Event%20Materials/2016-04%20-%20OP%20Spring%20Compliance%20Workshop%20(April%202012-14)/7.%20CIP-014-2%20Physical%20Security%20Site%20Visits.pdf).

<sup>38</sup> NERC, *Compliance Monitoring and Enforcement Program Quarterly Report, Q2 2017*, August 9, 2017, p. 8, <http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/Compliance%20Committee%20Open%20Meeting%20-%20August%209%202017.pdf>.

<sup>39</sup> NERC, email to CRS, February 14, 2018.

<sup>40</sup> NERC, December 7, 2017.

<sup>41</sup> NERC, February 14, 2018.



1998, the E-ISAC is the electricity sector's primary communications channel for security-related information, situational awareness, incident management, and coordination.<sup>42</sup> Among its key responsibilities, the E-ISAC gathers and analyzes security data, shares it with stakeholders, and communicates security risk mitigation strategies.<sup>43</sup> Bulk power entities are required to report physical security events to the E-ISAC under NERC's Event Reporting Reliability Standard (EOP-004), which was approved by FERC in 2013 and revised in 2015.<sup>44</sup>

Although operated by NERC, the E-ISAC is independent and organizationally separate from NERC's standards enforcement functions; information shared by utilities with the E-ISAC is not passed on to NERC compliance staff.<sup>45</sup> Nonetheless, the E-ISAC has played a role in facilitating industry understanding of physical security best practices. For example, the E-ISAC has added significant physical security threats and tactics to the NERC's biennial GridEx security exercises (discussed later in this report). In 2015, the E-ISAC also established a Physical Security Advisory Group, which includes industry physical security professionals, outside experts, and representatives from DOE and the Department of Homeland Security (DHS), to assist in the analysis of physical security threats and advise asset owners on physical threat mitigation. Through these efforts, the E-ISAC developed and ratified a design basis threat for the electric sector in December 2015.<sup>46</sup> The E-ISAC also has hosted two threat workshops, with plans for more.<sup>47</sup> Thus, while the E-ISAC has had no role in enforcing the CIP-014 standards, the security risk and mitigation information it develops and promulgates support the activities of bulk power asset owners complying with the standards.

## FERC Oversight

As the agency with general statutory authority over grid reliability, and the agency which ordered and approved NERC's CIP-014 standard, the Federal Energy Regulatory Commission also oversees implementation of the standard. In carrying out this oversight, FERC relies primarily on annual compliance reporting by NERC.<sup>48</sup> However the commission also conducts some independent compliance activities, and it also conducts some compliance activities in cooperation with NERC. For example, during the initial rollout of the CIP-014 standard in 2016, FERC staff coordinated with NERC staff in support of on-site visits to the covered entities discussed above.<sup>49</sup>

In its order approving CIP-014-01, the commission stated that NERC staff would submit to both the NERC Board of Trustees and FERC a report following implementation of requirements R1,

<sup>42</sup> ISACs for critical infrastructure sectors were established under Presidential Decision Directive 63, May 22, 1998. NERC operates the E-ISAC in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC). The ESCC, established in 2004 by companies in the electric power industry, coordinates policy-related activities involving the reliability and resilience of the sector, including physical and cyber infrastructure.

<sup>43</sup> NERC, *Understanding Your E-ISAC*, June 2016, p. 3.

<sup>44</sup> NERC, "EOP-004-3—Event Reporting," 2015, <http://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-3.pdf>.

<sup>45</sup> NERC, June 2016, p. 3.

<sup>46</sup> NERC, *State of Reliability 2016*, May 2016, p. 7.

<sup>47</sup> NERC, *State of Reliability 2017*, June 2017, p. 62.

<sup>48</sup> FERC, *Order on Electric Reliability Organization Reliability Assurance Initiative and Requiring Compliance Filing*, Docket No. RR15-2-000, p. 11, February 19, 2015, [http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/FERC\\_Order\\_Approving\\_Risk-Based\\_CMEP.pdf](http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/FERC_Order_Approving_Risk-Based_CMEP.pdf).

<sup>49</sup> NERC, May 2017, p. 16.

R2, and R3 about the scope, number, and characteristics of facilities identified as critical.<sup>50</sup> The order stated that

Based on the results reported by NERC, we expect Commission staff to audit a representative number of applicable entities to ensure compliance with Reliability Standard CIP-014-1. Depending on the audit findings, the Commission will determine if there is a need for any further action by the Commission including, but not limited to, directing NERC to develop modifications to Reliability Standard CIP-014-1 to provide greater specificity to the methodology for determining critical facilities.<sup>51</sup>

As of November 2, 2017, FERC had completed two audits of critical assets identified by covered entities (R1) and was in the process of conducting a third. These audits have involved technical review of utility regulatory documents by FERC engineers. According to FERC staff, the initial audits identified one issue of concern related to the interpretation of specific language in the standard regarding asset criticality.<sup>52</sup> In addition to NERC's annual reports, FERC receives from NERC periodic Notices of Penalty (NOP) to regulated entities for reliability standards violations. As of November 30, 2017, FERC received NOPs for two violations (apparently at the same utility) of the CIP-014 standard.<sup>53</sup>

## DOE Initiatives

Presidential Decision Directive 63 (PDD-63), issued during the Clinton Administration in 1998, established national policy for critical infrastructure protection from both physical and cyber threats.<sup>54</sup> PDD-63 established 15 critical infrastructure sectors. The Department of Energy was assigned responsibility for (1) the electric power, and (2) the oil and natural gas production and storage sectors. The George W. Bush Administration built on the work of PDD-63, superseding it in 2003 with Homeland Security Presidential Directive 7 (HSPD-7) on "Critical Infrastructure Identification, Prioritization, and Protection."<sup>55</sup> HSPD-7 again assigned to DOE (as a Sector-Specific Agency) responsibility for the energy sector—including electric power—as well as responsibility for being the federal coordinator for all critical infrastructure protection efforts.<sup>56</sup> The Obama Administration superseded HSPD-7 with Presidential Policy Directive 21 (PPD-21) on "Critical Infrastructure Security and Resilience" in 2013.<sup>57</sup> PPD-21 retained the Sector-Specific Agencies (SSAs) from HSPD-7, with DOE continuing as the SSA for the energy sector. Thus, DOE has had a supportive role in helping utilities to protect bulk power critical assets over the last two decades.

<sup>50</sup> FERC, *Physical Security Reliability Standard*, Docket No. RM14-15-000, Order No. 802, November 20, 2014, p. 23, <http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Final%20Rule%20on%20CIP-014-1.pdf>.

<sup>51</sup> FERC, Order No. 802, p. 24.

<sup>52</sup> FERC, Staff meeting with CRS analysts, Washington, D.C., November 2, 2017.

<sup>53</sup> NERC, *Enforcement and Mitigation*, "Searchable NOP Spreadsheet," web page, accessed December 12, 2017, <http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx>.

<sup>54</sup> National Security Council and National Security Council Records Management Office, "PDD-63—Critical Infrastructure Protection," *Clinton Digital Library*, May 20, 1998.

<sup>55</sup> George W. Bush White House Archives, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive/HSPD-7, December 17, 2003.

<sup>56</sup> For details about the roles of Sector-Specific Agencies, see Department of Homeland Security, "Sector-Specific Agencies," web page, July 11, 2017, <https://www.dhs.gov/sector-specific-agencies>.

<sup>57</sup> Barack H. Obama White House Archives, "Critical Infrastructure Security and Resilience," Presidential Policy Directive-21, February 12, 2013.

Until recently, DOE's power grid security activities were led by its Office of Electricity Delivery and Energy Reliability (OE) within the Office of the Under Secretary for Science and Energy. A 2008 OE report stated that "OE's mission is to advance technology—in partnership with industry, government, academia, and the public—to meet America's need for a reliable, efficient, and resilient electric power grid."<sup>58</sup> Although the office was primarily focused on grid cybersecurity, it did conduct activities related to power grid physical security, including analysis of large power transformer security, a substation security awareness campaign, and efforts to support and coordinate research and development for physical security.<sup>59</sup> On February 14, 2018, DOE announced that the Secretary of Energy was establishing a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to be led by an Assistant Secretary with responsibilities to help protect energy infrastructure from "from cyber threats, physical attack and natural disaster."<sup>60</sup> How this reorganization will affect DOE's activities in bulk power physical security remains to be seen.

## Observed Changes in Bulk Power Physical Security

Most grid security analysts consider the 2013 Metcalf substation attack to have been the "wake up call" which both changed electric sector attitudes toward grid physical security and motivated the promulgation of NERC's physical security regulations. Since that time, there have been a number of apparent changes within the electricity sector related to increasing bulk power physical security. It is not clear whether these changes have been driven more by changes in utility perceptions of grid threats or by NERC's mandatory security standards. Furthermore, there is currently no comprehensive accounting of changes in physical security throughout the sector. Nonetheless, anecdotal information in the public domain suggests that such changes may be significant and widespread. They are discussed in the following sections.

## Corporate Structure Supporting Physical Security

One criticism that arose in the wake of the Metcalf attack was that physical security management at Pacific Gas and Electric Company (PG&E, the Metcalf substation's owner) and at other utilities was not a centrally organized or well-supported function in corporate management. This lack of support limited the influence of security managers in corporate planning and financial decisions.<sup>61</sup> However, it appears that many utilities have been reconfiguring and elevating physical security functions within their corporate structures. For example, owners of transmission assets such as PG&E, American Electric Power, and Xcel Energy have appointed Chief Security Officers at senior levels responsible for managing both physical and cyber security risks company-wide.<sup>62</sup>

<sup>58</sup> Department of Energy, Office of Electricity Delivery and Energy Reliability (Hereinafter OE), *National SCADA Test Bed Program, Multi-Year Plan FY2008-2013*, January 2008, p. 7.

<sup>59</sup> Department of Energy, Energy Sector-Specific Plan, 2015, pp. 16, 27. For discussion of OE's cybersecurity activities, see CRS Report R44939, *Cybersecurity for Energy Delivery Systems: DOE Programs*, by Paul W. Parfomak, Chris Jaikaran, and Richard J. Campbell.

<sup>60</sup> U.S. Department of Energy, "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response," press release, February 14, 2018.

<sup>61</sup> See, for example: Tony Kovalesski, Liz Wagner, and Mark Villarreal, "Internal Memo Reveals PG&E Years Away from Substation Security," *NBC Bay Area*, April 5, 2106, <https://www.nbcbayarea.com/investigations/Internal-Memo-Reveals-PGE-Years-Away-from-Substation-Security-303833811.html>.

<sup>62</sup> PG&E Corp., "Bernard A. Cowens," web page, January 9, 2017, <http://www.pgecorp.com/corp/about-us/officers/> (continued...)

The senior security professional, typically at the vice president or director level, now has direct access to the [Chief Executive Officer] and company boards of trustees, often to supply situational awareness of physical and cybersecurity issues.... The electricity industry is quickly moving away from security as an “addition duty”.... [M]ost utilities today have dedicated security departments committed to the protection of company assets and personnel.<sup>63</sup>

Utilities are also centralizing and bolstering their physical security capabilities at the operational level. Between 2014 and 2017, for example, Xcel Energy consolidated and grew its staffing for the “Chief Security Officer class of services” from 47 to 63 employees.<sup>64</sup> According to the company’s regulatory filings,

the increase in average staffing levels.... was due to the need to correct a lack of resources to ensure adequate headcount to provide essential cyber and physical Enterprise Security services for Xcel Energy.... This increase in staffing demonstrates the emerging need that led to a stand-alone organization (i.e., the Chief Security Officer) to focus on Cyber Operations, Enterprise Resilience, Physical Security and Security Governance.<sup>65</sup>

Likewise, in response to the Metcalf attack, Dominion Energy established “a true cross-functional team with more than 100 people representing the entire Dominion organization,” to develop and implement a more comprehensive substation security program.<sup>66</sup> Such efforts appear to extend to major publicly owned utilities as well. For example, according to the head of the Western Area Power Administration (WAPA), one of four federal power marketing administrations,

WAPA’s approach to physical security.... began in 2013 with the consolidation of our Office of Security and Emergency Management across our five regions and the implementation of a sophisticated risk-based program in analyzing the threats and vulnerabilities to our substations.<sup>67</sup>

The Tennessee Valley Authority (TVA), which operates federally-owned hydroelectric and nuclear generation and associated transmission assets, recently closed a job posting for eight entry-level Inspectors, each to be “trained as a physical security specialist” to provide “comprehensive security services, including assessments of facilities to identify credible threats, and implementation and testing of countermeasures to mitigate risks.”<sup>68</sup>

---

(...continued)

company/bernard-cowens.page; American Electric Power, “AEP Names Partlow Vice President & Chief Security Officer,” press release, August 25, 2015; Xcel Energy, *Application of Southwestern Public Service Company for Authority to Change Rates*, Direct Testimony of Stephen J. Brown, filing with the Public Utility Commission of Texas, August 21, 2017, <https://www.xcelenergy.com/staticfiles/xe-responsive/Company/Rates%20&%20Regulations/Rate%20Cases/Brown-RR-Direct.pdf>.

<sup>63</sup> Brian Harrell, “The Modern Look of a Utility’s Chief Security Officer,” *CSO*, August 4, 2016, <https://www.csoonline.com/article/3101474/leadership-management/the-modern-look-of-a-utilitys-chief-security-officer.html>.

<sup>64</sup> Xcel Energy, *Application of Southwestern Public Service Company for Authority to Change Rates*, Update Testimony of Stephen J. Brown, September 27, 2017, p. 10, <https://www.xcelenergy.com/staticfiles/xe-responsive/Company/Rates%20&%20Regulations/Rate%20Cases/13%20-%20BrownRRUpdate.pdf>.

<sup>65</sup> Xcel Energy, August 21, 2017, p. 26.

<sup>66</sup> Bob McGuire, et al., “Substation Security Is More Than Just a Fence,” *T&D World*, September 28, 2015.

<sup>67</sup> Mark A. Gabriel, Administrator and Chief Executive Officer, Western Area Power Administration, “Physical and Cyber Threats,” *T&D World*, May 8, 2017. Power Marketing Administrations (PMAs) operate electric transmission systems and sell power generated by federally-owned hydroelectric dams across much of the United States.

<sup>68</sup> Tennessee Valley Authority, “Inspector I – 507038,” job posting, *Linked-in JOBS*, web page, posted January 17, 2018, accessed February 1, 2018, <https://www.linkedin.com/jobs/view/inspector-i-507038-at-tennessee-valley-> (continued...)

Some transmission owners are also specifically increasing their in-house intelligence capabilities in physical security, including recent postings for positions such as “Security Intelligence Specialist” and “Director—Corp Security Info & Intelligence.”<sup>69</sup> While the examples above are anecdotal, they would be consistent with what may be a trend among key grid owners to make physical security a better-organized and more influential corporate function. Not all utilities may be implementing such organizational changes, however.

## Physical Security in Long-Term Transmission Planning

Since NERC promulgated the CIP-014 standards, some utilities have begun to put a greater emphasis on bulk power physical security as a design consideration in long-term transmission system planning. This approach aligns with the California Public Utilities Commission’s recommendation in its 2018 report that, “there should be an emphasis on incorporating a menu of physical security strategies [into] any substation from the time of its inception.”<sup>70</sup> For example, Public Service Enterprise Group’s transmission planning criteria for its Long Island system in New York discusses the use of power system simulation tools for “various transmission system security and reliability studies.”<sup>71</sup> Commonwealth Edison’s transmission planning criteria includes a separate section on “security criteria” for system design which considers “severe low probability outage combinations” and seeks “to avoid cascading outages, instability, or widespread blackout.”<sup>72</sup> Such criteria could apply to both natural and man-made outages, but they are consistent with, and readily applied to, design considerations for enhanced physical security. American Electric Power (AEP) also has incorporated asset criticality as a design criterion in its transmission planning.

As a result of the revised NERC CIP standards, AEP now classifies all of its bulk electric system facilities based on the critical nature of the equipment to determine the level of security needed. This approach allows us to design security controls directly into new infrastructure from the start, building the costs into capital projects as needed. It also allows us to be more proactive with new and existing infrastructure while balancing risks with mitigation solutions.<sup>73</sup>

In its plans for a 2018 reliability-related upgrade at one its substations, Vermont Electric Power Company states that it “will also take the opportunity to make improvements to the physical security” of the substation.<sup>74</sup> According to NERC officials, based on security criteria, some

---

(...continued)

authority-578188690.

<sup>69</sup> American Transmission Company, “Security Intelligence Specialist,” job listing on *LinkedIn*, posted March 6, 2017, <https://www.linkedin.com/jobs/view/security-intelligence-specialist-at-american-transmission-552328921>; Avangrid, “Director—Corp Security Info & Intelligence,” job listing on *Glassdoor.com*, posted January 3, 2018, [https://www.glassdoor.com/job-listing/director-corp-security-info-intelligence-avangrid-JV\\_IC1148470\\_KO0,40\\_KE41,49.htm?jl=2630675613&utm\\_source=google\\_jobs&utm\\_medium=organic](https://www.glassdoor.com/job-listing/director-corp-security-info-intelligence-avangrid-JV_IC1148470_KO0,40_KE41,49.htm?jl=2630675613&utm_source=google_jobs&utm_medium=organic).

<sup>70</sup> CPUC, January 2018, p. 8.

<sup>71</sup> PSEG Long Island, “Transmission Planning Criteria,” accessed January 10, 2018, p. 5, <https://www.psegliny.com/files.cfm/TransmissionPlanningCriteria.pdf>.

<sup>72</sup> Commonwealth Edison Co., “Transmission Planning Criteria,” February 10, 2017, p. 10, <https://www.pjm.com/-/media/planning/planning-criteria/commonwealth-edison-planning-criteria.ashx?la=en>

<sup>73</sup> American Electric Power Corp., *2017 AEP Corporate Accountability Report*, “Cyber and Physical Security,” web page, May 25, 2017, <http://www.aepsustainability.com/about/security/cyber.aspx>.

<sup>74</sup> Vermont Electric Power Company, “East Avenue & Queen City Substation Improvement Project,” web page, accessed February 1, 2018, <https://www.velco.com/our-work/projects/project-east-avenue-queen-city-substation-improvement-project>.



utilities also have begun to consider new transmission interconnections not only to increase line capacity for bulk power flows, but also to reduce the criticality of particular transformer substations in congested areas by providing more transmission paths around them.<sup>75</sup>

## New Security Products and Services

As utilities have devoted greater organizational and financial resources towards power grid physical security, industry vendors have been offering more physical security products and services to meet sector demand. As one utility services company has observed, “we can expect plenty of innovation as manufacturers see new markets due to the new standards for physical security of critical substations.”<sup>76</sup> These offerings range from analytical services for security planning to physical products to harden physical assets. A comprehensive survey of such offerings is beyond the scope of this report, but the following examples illustrate the kinds of products now commercially available in the bulk power physical security market.

- **Security Program Planning and Implementation.** Engineering and security consulting firms have developed customizable programs specifically for power grid physical security review, planning, analysis, and implementation in compliance with the CIP-014 standards and utility-specific requirements.<sup>77</sup>
- **Anti-Intrusion Products.** Vendors have been marketing existing intrusion-related products specifically for use at bulk power critical facilities. These products include visual, acoustic, thermal radar, and electromagnetic systems for facility monitoring, intrusion detection, and response.<sup>78</sup>
- **Hardened Transformers and Components.** At least two major manufacturers have been marketing bulk power transformers with integrated ballistic shielding, or customizable plates to shield existing transformers.<sup>79</sup> Smaller manufacturers have also begun marketing hardened transformer components, such as composite bushings, for new and retrofit substation applications.<sup>80</sup>
- **Substation Perimeter Shielding.** A number of vendors have been marketing perimeter fencing and wall products specifically for visual and physical shielding of bulk power substations.<sup>81</sup> Most of these products are designed specifically to protect against rifle attacks such as the Metcalf attack.

---

<sup>75</sup> NERC, December 7, 2017.

<sup>76</sup> Southwire Company, “Protecting the Grid,” *T&D World*, sponsored content, May 15, 2017.

<sup>77</sup> See, for example: Burns & McDonnell, “Station Defender,” web page, January 30, 2018, <https://info.burnsmcd.com/station-defender/project-delivery>; Corporate Risk Solutions, “Physical Security,” web page, January 30, 2018, <https://corprisk.net/physical-security/>.

<sup>78</sup> See, for example: “How VTI Security Protected an Electrical Substation With a Radar-Thermal Imaging Solution,” *Security Sales & Integration*, September 20, 2017, <https://www.securitysales.com/in-depth/vti-security-radar-thermal-imaging-solution/>; and i2c Technologies, Ltd., “Power Substation Protection,” marketing brochure, May 2017, <http://www.i2ctech.com/wp-content/uploads/2017/05/2509-i2cTech-CMYK.pdf>.

<sup>79</sup> See, for example: Siemens AG, “First Bullet Resistant Retrofit Ordered for a Transformer,” press release, accessed January 28, 2018, <https://www.siemens.com/global/en/home/products/energy/references/first-bullet-resistant-retrofit-ordered-for-a-transformer.html>.

<sup>80</sup> Mike Sheppard and Saqib Saeed, “Bullet and Weather Concerns Driver of Retrofits in US Market,” Power Technology Research LLC, October 26, 2017, <https://powertechresearch.com/bullet-and-weather-concerns-driver-of-retrofits-in-us-market/>.

<sup>81</sup> See for example: Oldcastle, Inc., “How Precast Substation Walls Increase Power Grid Security,” web page, <https://www.buildingsolutions.com/industry-insights/how-precast-substation-walls-increase-power-grid-security>; (continued...)

Although new physical security products and services are being marketed in the utility sector, there is no comprehensive source of data about their sales to bulk power asset owners. Simply because vendors are marketing products does not mean that many utilities are buying them. For example, as of October 2017, Siemens Corp. had announced only one commercial order for its new transformer ballistic shielding retrofit product.<sup>82</sup> Thus, the overall impact of such offerings on the sector cannot be qualified reliably. Additional discussion of physical security spending is in the following section.

## Capital Investment in Physical Security

Major changes in power grid operational expenses and capital investment are generally slow to occur. In privately owned utilities, significant changes in spending and plans for new capital projects may need to go through a number of rigorous screens, including power network modeling, a corporate capital allocation process, a regulatory approval process, and a procurement process. Publicly owned utilities may need approval from cooperative boards, or municipal or federal officials. This combination of requirements can take years to complete. Consequently, many significant operating expenditures or capital investments for physical security identified in security plans under CIP-014 may still be working their way through utility budgets and implementation. For example, in a 2016 rate filing, Southern California Edison stated that it planned to make physical security improvements at approximately 24 facilities in 2015-2017 and proposed to upgrade 8 substations per year from 2016 through 2020.<sup>83</sup> Likewise, in its 2016 annual report, Dominion Resources' timeline for power grid capital investment in "Physical Security" runs to 2021.<sup>84</sup>

Notwithstanding the potential length of time it may take for some security projects to be approved and implemented, there are indications in the public record that bulk power asset owners have already been spending more on new physical security measures. In its December 2016 report, the Edison Electric Institute stated that "primary factors driving transmission investment between 2015 and 2019" included "system hardening and resiliency to minimize adverse catastrophic events" and "improvements to comply with evolving transmission reliability and security compliance standards."<sup>85</sup> In its January 2018 white paper, the California Public Utilities Commission (CPUC) reports that investor-owned utilities under its jurisdiction "already ... have sought approval for tens of millions of dollars in General Rate Case funding to ensure physical security."<sup>86</sup> The following examples illustrate the types of physical security projects and recent spending in publicly available sources.

---

(...continued)

AFTEC LLC, "Substation Security Walls," web page, 2017, <https://aftec.com/substation-security-walls/>;

<sup>82</sup> Siemens AG, "First Bullet Resistant Retrofit Ordered for a Transformer," press release, October 17, 2017, <https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/energy-management/medium-voltage-power-distribution/2017-10-17-tr-success-bullet-resistant-retrofit-v1-en.pdf>.

<sup>83</sup> Southern California Edison Co., Application Of Southern California Edison Company (U 338E) For Authority To Increase Its Authorized Revenues For Electric Service In 2018, Among Other Things, And To Reflect That Increase In Rates, A.16-09-001, Before the Public Utilities Commission of the State of California, September 1, 2016, [http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/9F664E3F0B77B7E488258195007C8F53/\\$FILE/SCE%20Opening%20Brief%20and%20COS.pdf](http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/9F664E3F0B77B7E488258195007C8F53/$FILE/SCE%20Opening%20Brief%20and%20COS.pdf).

<sup>84</sup> Dominion Resources, Inc., *Energy is Essential*, 2016 Summary Annual Report, 2017, p. 5.

<sup>85</sup> Edison Electric Institute, *Transmission Projects: At A Glance*, December 2016, p. vi.

<sup>86</sup> California Public Utilities Commission (CPUC), *Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699*, January 2018, p. 5.

- In 2017, the Bonneville Power Administration announced stand-alone plans to install security fencing at two high-voltage substations in compliance with NERC's security standards and to "protect critical assets from theft, vandalism, and terrorism."<sup>87</sup>
- In 2017, PPL Electric Utilities reportedly filed for regulatory approval for a \$450,000 expenditure to reconfigure a 500 kV substation in compliance with NERC's CIP-014 physical security standard.<sup>88</sup>
- In 2017 regulatory filings, Vectren (Indiana) described plans to invest \$2.9 million for physical security upgrades at critical substations, including enhanced fencing, access control, video surveillance, and perimeter motion detection.<sup>89</sup>
- According to the Western Area Power Administration, its expenses for physical security "nearly tripled" between 2013 and 2017.<sup>90</sup>

## Utility Participation in Voluntary Security Programs

Although the CIP-014 mandatory physical security standards have only been in effect since 2014, bulk power asset owners have had earlier opportunities to participate in voluntary security initiatives administered by NERC and DHS. Utility participation in these voluntary programs is another indication of overall efforts in the sector to improve critical asset physical security.

## NERC Grid Security Exercises

In 2011, NERC conducted GridEx, the first of an ongoing series of biennial electric sector-wide grid security exercises.<sup>91</sup> The 2011 exercise assessed the readiness of utilities to respond to a cyberattack, strengthened their crisis response, and provided input for internal security program improvements. Although the exercise was focused on a cyberattack, it did involve physical incursions into power grid substations as well as aspects of grid monitoring and recovery that would be relevant to an attack on critical transformers.<sup>92</sup> After the Metcalf attack in 2013, NERC conducted a second, more expansive grid security exercise, GridEx II. The exercise scenario included a cyberattack on the grid coupled with a coordinated physical attack against a subset of transmission and generation assets—including critical transformer substations.<sup>93</sup> NERC conducted GridEx III in 2015, again including a baseline scenario with cyber and physical

<sup>87</sup> Bonneville Power Administration, Categorical Exclusion Determination, "Proposed Action: Covington and Maple Valley Substations Perimeter Security Upgrades," April 27, 2017, [https://www.bpa.gov/efw/Analysis/CategoricalExclusions/cx/20170427\\_Covington-and-Maple-Valley-Substations-Perimeter-Security-Upgrades.pdf](https://www.bpa.gov/efw/Analysis/CategoricalExclusions/cx/20170427_Covington-and-Maple-Valley-Substations-Perimeter-Security-Upgrades.pdf).

<sup>88</sup> Corina Rivera Linares, "PPL Electric Utilities Seeks Approval of Two Projects in Pennsylvania," *Transmission Hub*, PennWell Publishing, May 22, 2017.

<sup>89</sup> Southern Indiana Gas and Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc. IURC Cause No. 44910, filing with the Indiana Utility Regulatory Commission, February 23, 2017, Attachment LKW-2, p. 31, [https://iurc.portal.in.gov/\\_entity/sharepointdocumentlocation/b4477c28-00fa-e611-8104-1458d04e8ff8/bb9c6bba-fd52-45ad-8e64-a444aef13c39?file=44910\\_Vectren%20South\\_No%202\\_Direct%20Testimony%20and%20Attachments\\_Wilson\\_PUBLIC\\_022317.pdf](https://iurc.portal.in.gov/_entity/sharepointdocumentlocation/b4477c28-00fa-e611-8104-1458d04e8ff8/bb9c6bba-fd52-45ad-8e64-a444aef13c39?file=44910_Vectren%20South_No%202_Direct%20Testimony%20and%20Attachments_Wilson_PUBLIC_022317.pdf)

<sup>90</sup> Mark A. Gabriel, May 8, 2017.

<sup>91</sup> NERC's E-ISAC division organizes and administers its GridEx exercises.

<sup>92</sup> North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. i.

<sup>93</sup> NERC, *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.15; Matthew L. Wald, "Attack Ravages Power Grid. (Just a Test.)," *New York Times*, November 14, 2013.

attacks, but also with an option for participants to customize the baseline scenario to meet local objectives.<sup>94</sup> NERC conducted its most recent exercises, GridEx IV, in November 2017.

According to NERC, one indication of progress in bulk power grid security is increasing participation by electricity sector entities in its GridEx exercises. The number of utilities participating in GridEx rose from 49 in 2011 to 166 in 2015.<sup>95</sup> NERC has not yet released participation details for GridEx IV, but the DOE reported that the latest exercise had more participants than in 2015.<sup>96</sup>

## DHS Critical Infrastructure Surveys

The Department of Homeland Security's Protective Security Coordination Division conducts voluntary field assessments of critical infrastructure to identify vulnerabilities, interdependencies, capabilities, and cascading effects of potential terrorist attacks. As part of these efforts, DHS Protective Security Advisors offer voluntary, web-based security surveys of critical facility security using the agency's Infrastructure Survey Tool developed in 2008. The key goals of the surveys are to identify facilities' physical security and security management, identify security gaps, create facility protective and resilience measures indices that can be compared to similar facilities, and track progress toward improving security.<sup>97</sup> According to DHS officials, of more than 6,000 surveys completed since the program began, over 600 have been conducted on electric power facilities—although the timing of these surveys and the specific types of power facilities involved are not reported.<sup>98</sup>

## Legislative Proposals in the 115<sup>th</sup> Congress

Given the relatively recent promulgation of NERC's new physical security standards, bulk power physical security has not been a major legislative focus in the 115<sup>th</sup> Congress. Nonetheless, several bills include provisions intended to enhance bulk power physical security—primarily by establishing new DOE grid security programs rather than by imposing new requirements on FERC or on bulk power asset owners directly. The relevant provisions of these bills, and a related resolution, are summarized below.

- **The Enhancing Grid Security Through Public-Private Partnerships Act** (H.R. 5240) would require DOE to establish a program to facilitate public-private partnerships for electric utility physical security and cybersecurity, among other provisions. Program activities would support voluntary implementation of maturity models, self-assessment, and security auditing; sharing of best practices and data collection in the electric sector; and training and technical assistance to utilities (§2(a)).

<sup>94</sup> NERC, *Grid Security Exercise: GridEx III Report*, March 2016, p. 7.

<sup>95</sup> NERC, March 2016, p. 1.

<sup>96</sup> U.S. Department of Energy, "GridEx IV: Government and Industry Exercise Together to Improve the Response to Grid Security Emergencies," November 21, 2017, <https://energy.gov/articles/gridex-iv-government-and-industry-exercise-together-improve-response-grid-security>.

<sup>97</sup> Department of Homeland Security, "Critical Infrastructure Vulnerability Assessments," web page, April 17, 2017, <https://www.dhs.gov/critical-infrastructure-vulnerability-assessments>.

<sup>98</sup> Daniel Genua, Department of Homeland Security, Presentation at George Mason University, Center for Energy Science and Policy, Grid Security Symposium, Arlington, VA, October 25, 2017, [http://cesp.gmu.edu/wp-content/uploads/2017/10/UNCLASS\\_GMU-Panel-Presentation\\_25Oct2017\\_FINAL.pdf](http://cesp.gmu.edu/wp-content/uploads/2017/10/UNCLASS_GMU-Panel-Presentation_25Oct2017_FINAL.pdf).

- The **Energy Emergency Leadership Act** (H.R. 5174) would amend the Department of Energy Organization Act to include “energy emergency and energy security” to the functions assigned to Assistant Secretaries. These functions would include responsibilities with respect to emerging threats, supply, and emergency planning, among others. They would also include “provision of technical assistance, support, and response capabilities with respect to energy security threats, risks, and incidents” (§2).
- The **Energy and Natural Resources Act of 2017** (S. 1460) would require DOE to develop an advanced energy security program to secure energy networks, including electric transmission and delivery. Eligible activities would include developing “capabilities to identify vulnerabilities and critical components that pose major risks to grid security if destroyed or impaired,” modeling national level impacts from human-made events, developing a physical security maturity model, conducting grid security exercises, conducting research on critical asset hardening, and other related measures (§2002(e)).
- The **Leading Infrastructure for Tomorrow’s America Act** (H.R. 2479) would establish a grant program administered by DOE “to enhance energy security through measures for electricity delivery infrastructure hardening and enhanced resilience and reliability” (§31101(a)).
- The **Advancing Grid Storage Act of 2017** (S. 1851) would establish a competitive grant program for pilot energy storage systems administered by DOE with one objective being to “improve the security of critical infrastructure and emergency response systems” in the electric grid (§5(a)(4)(A)).
- The **Grid Cybersecurity Research and Development Act** (H.R. 4120) would require DOE, together with bulk power asset owners, and in collaboration with the National Laboratories, to “utilize a range of methods, including voluntary vulnerability testing and red team-blue team exercises, to identify vulnerabilities in physical and cyber systems” (§6(a)).
- The **Flexible Grid Infrastructure Act of 2017** (S. 1875) would require DOE to: develop model standards for the electric distribution grid, in part to improve security with respect to physical threats (§5(d)(1)), evaluate whether new performance standards and testing procedures are needed to ensure electrical equipment resilience in the face physical threats (§5(d)(2)), and submit to Congress methods and guidelines for calculating the costs and benefits of investments in resilience and security solutions for the electric grid (§5(e)(1)).
- **House Resolution 334** states that it should be the policy of the United States to, among other things, “bolster the reliability, affordability, diversity, efficiency, security, and resiliency of domestic energy supplies, through advanced grid technologies,” and to promote advanced grid tools “to increase data security, physical security, and cybersecurity awareness and protection.”

## Policy Issues for Congress

Although NERC’s CIP-014 standards have been promulgated, and bulk power asset owners have begun enhancing physical security, Congress continues to be concerned about the current state of electric grid physical security. Among many issues of potential interest, Congress may focus on several with overarching policy significance: security implementation oversight, cost recovery, hardening vs. resilience, and the quality of threat information.



## Oversight of Physical Security Implementation

Although FERC's statutory authority for grid reliability and NERC's reliability standards both include provisions for oversight and enforcement, congressional oversight of physical security implementation may be a challenge for several reasons. First and foremost, information about physical security measures is inherently sensitive and there are both statutory and regulatory restrictions on its disclosure.<sup>99</sup> Therefore, the level of security-related information that utilities are willing or able to provide outside the CIP-014 third-party review process or NERC compliance audits is more limited than reports about, say, general reliability or safety.

NERC is not compiling a centralized database of critical assets or security measures implemented by the utilities subject to its physical security standard. Moreover, while NERC may provide security information to FERC, the security-related information NERC can provide in public reports is limited and typically redacted. Therefore, although information about CIP-014 implementation exists among the utilities and independent third parties (operating within the standard), and is provided at some level of specificity to NERC, that information may not be as useful or visible as it could be to Congress or other outside entities.

Another oversight challenge arises because NERC's CIP-014 standards are not prescriptive; bulk power asset owners have considerable discretion in the nature and timing of the physical security measures they may include in their physical security plans. NERC viewed such flexibility as necessary for its standard due to the unique characteristics of each utility's bulk power system and the risks it faces. However, this flexibility also may make it more difficult to develop useful metrics for CIP-014 implementation and comparing implementation among asset owners. NERC's standards for power grid physical security may ensure considerable consistency in the *process* utilities must undertake to identify critical substations and develop plans to secure them. However, they may not ensure consistency among the various security plans nor in the specific measures the individual asset owners will choose to implement to reduce the risk of intentional attacks. For example, ballistic shielding at critical substations may be an appropriate and sufficient protective measure for some utility assets, say, in open and rural areas, but not necessarily in more urban areas.

Even when detailed company-specific information about physical security measures is available, it might be difficult to develop reliable metrics to evaluate it. Metrics are an important tool NERC uses to evaluate utility performance in the context of power grid reliability.<sup>100</sup> However, officials at EEI have stated that measuring the adequacy of grid security for a diverse set of asset owners under changing risk circumstances poses significant problems. "Security metrics (for both cyber and physical security) have consistently been a challenge due evolving threats and vulnerabilities. If you build an eight-foot fence, the attacker just needs to bring a nine-foot ladder."<sup>101</sup> NERC is actively engaged in efforts to develop bulk power system security metrics in which it has likewise encountered "challenges associated with developing relevant and useful security metrics that rely on data willingly and ably provided by individual entities."<sup>102</sup>

---

<sup>99</sup> FERC regulations for the submission, designation, handling, sharing, and dissemination Critical Energy/Electric Infrastructure Information (CEII) are at 18 C.F.R. § 388.113.

<sup>100</sup> See NERC, "Reliability Indicators," web page, <http://www.nerc.com/pa/RAPA/Pages/ReliabilityIndicators.aspx>.

<sup>101</sup> Chris Hickling, Edison Electric Institute, "RE: CIP-014 Implementation Update," email to CRS, October 30, 2017.

<sup>102</sup> NERC, *State of Reliability 2017*, June 2017 p. vii. For an expansive discussion of NERC's efforts to develop security metrics, see Appendix G in this NERC report.

Congress may judge the effectiveness of the CIP-014 physical security standards as best it can based on reports and testimony from NERC and FERC as well as information from the assets owners themselves. However, due to the issues above, if Congress decides the information as currently structured is insufficient to draw reliable conclusions about the status of bulk power physical security as a whole, it may revisit how the responsible agencies collect, measure, and report it. Congress may also consider additional avenues for reviewing this information, for example, through classified briefings or specifically requested studies or reports. Also, as FERC continues to implement its policy of regulating physical security of the power grid, Congress may examine whether company-specific security initiatives appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid overall uniformly reflect terrorism risk from a national perspective.

## Financial Requirements and Cost Recovery

Two of the barriers to physical security investment among utilities prior to the Metcalf attack were competition for limited capital investment resources and justifying security spending to corporate boards and utility rate regulators. NERC regulatory requirements for physical security make it easier for security managers to justify related operating and capital expenditures to corporate leadership, and to seek cost recovery for such expenditures through regulated rates. However, even where regulators have been supportive of cost recovery for physical security investments in general, they have faced challenges gauging the prudence of specific security investments because they are hard to evaluate on a traditional benefit-cost basis. As a 2006 report from the Electric Power Research Institute states,

Security measures, in themselves, are cost items, with no direct monetary return. The benefits are in the avoided costs of potential attacks whose probability is generally not known. This makes cost-justification very difficult.<sup>103</sup>

Note that cost-justification requires not only the approval of utility management, but also of FERC and potentially state public utility commissions which regulate the rates grid owners may charge for electric transmission and distribution service. Regulators are responsible for ensuring that electricity rates are just and reasonable. They must be convinced that any new grid security capital costs and expenses are necessary and prudent before they will allow them to be passed through to ratepayers. However, corporate financial processes differ from utility to utility, and utility rate regulation differs from jurisdiction to jurisdiction, so investment and cost recovery for physical security is not uniform across the electricity sector and remains a work in progress. As implementation of new physical security plans under CIP-014 continues, Congress may examine whether the overall level of investment appropriately reflects the level of security risk facing the bulk power system, and whether any cost-recovery barriers are preventing assets owners from making investments necessary to secure the grid.

## Hardening vs. Resilience

There are two fundamental approaches to reducing the risk of a successful physical attack on the electric grid. The first approach, which is the principal approach of NERC's CIP-014 standards, is to prevent attacks by monitoring critical facilities to identify would-be attackers before they attempt an attack, preventing attacker access to critical assets, and otherwise hardening facilities

---

<sup>103</sup> Electric Power Research Institute (EPRI), *Technologies for Remote Monitoring of Substation Assets: Physical Security*, March 2006, p. viii.

to make them more physically secure to protect against attack and equipment failure. The second approach is to make the broader power system more “resilient” to a successful attack on particular assets through an enhanced ability to manage loads, reroute power flows, and access other sources of generation to reduce the potential of blackouts even if critical assets are disabled.<sup>104</sup> Initiatives such as the spare transformer program administered by the Edison Electric Institute (EEI, the electric utility trade association), and a proposed federal Strategic Transformer Reserve, which can accelerate replacement of critical transformers if they are damaged, may contribute to the power grid’s ability to sustain a terrorist attack without widespread grid failure.<sup>105</sup> Thus, while hardening is aimed more at reducing the likelihood of a successful attack, resilience aims at reducing potential consequence; doing either reduces overall security risk.

Measures to harden critical facilities and measures to increase system resilience are not exclusive of one another. In fact, they can be complementary in reducing overall security risk. However, they may involve different approaches to power grid operation and design, and they may involve different, competing types of investment (e.g., transformer shielding vs. transmission network sensors). Balancing the two approaches to most efficiently achieve a desired level of physical security is a challenge for utilities with limited capital budgets. The CPUC stated that “determining appropriate security measures or approaches to ensuring resiliency” was one of three “major issues” in its power grid physical security proceedings.<sup>106</sup> As Congress continues its oversight of bulk power physical security regulation, it may consider whether the electric power sector as a whole is striking an appropriate balance between these two approaches.

## Threat Information

The utility industry’s physical security risk assessments rely upon threat information from the federal government, among other sources.<sup>107</sup> The quality of this threat information is a key determinant of what bulk power asset owners need to be protecting against and what security measures to take. Incomplete or ambiguous threat information may lead to inconsistency in physical security among grid owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat.

As discussed earlier in this report, the E-ISAC plays a valuable role in identifying and analyzing physical security risk, and disseminating information about those risks to bulk power asset owners. Independent third-party verification of risk assessments under the CIP-014 standards, together with NERC compliance audits, are two additional means of helping to ensure greater consistency of threat information among utilities. Nonetheless, a changing threat environment continues to pose challenges for physical security planning and investment. As NERC stated in a

<sup>104</sup> For a discussion about power grid resiliency and associated federal efforts, see *Government Accountability Office, Electricity: Federal Efforts to Enhance Grid Resilience*, GAO-17-153, January 2017.

<sup>105</sup> For details about electric sector spare transformer programs, see Department of Energy, *Strategic Transformer Reserve*, report to Congress, March 2017.

<sup>106</sup> CPUC, January 2018, p. 5.

<sup>107</sup> Much of this information is communicated primarily through the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the sector’s communications channel for security-related information, situational awareness, incident management, and coordination. The ES-ISAC was established under Presidential Decision Directive 63, May 22, 1998. The ES-ISAC is operated by NERC in collaboration with the DOE and Electricity Subsector Coordinating Council. Members may anonymously share information by means of a secure Internet portal. Registered users receive information on security threats and alerts, remediation, task forces, events, and other security-specific resources.

recent compliance report, “the security threat landscape is constantly changing and requires adaptation and information sharing on how best to address these issues in an effective and efficient manner.”<sup>108</sup>

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.<sup>109</sup> Threat information continues to be an uncertainty in the case of power grid physical security. For example, although there is wide consensus that the Metcalf attack was extremely alarming, some industry analysts have opined that FERC’s physical security order nonetheless may have been an “overreaction” to Metcalf.<sup>110</sup> By contrast, former DHS Secretary Michael Chertoff has predicted that “the sophistication and resulting damage of the Metcalf attack will ... be exceeded” in a future attack.<sup>111</sup> Still others have expressed concern that FERC’s physical security concerns may be too heavily focused on another Metcalf-type scenario—the last threat—rather than a wider range of potential future threats.

As discussed earlier, there is widespread belief that bulk power critical assets are vulnerable to physical attack, that such an attack potentially could have catastrophic consequences, and that the risks of such attacks are growing. But the exact nature of such potential attacks and the capability of perpetrators to successfully execute them are uncertain. Consequently, despite the technical arguments, with limited information about potential targets and attacker capabilities, the true vulnerability of the grid remains an open—and evolving—question. As Congress seeks to establish the best policies to address bulk power physical security, it may examine how federal and electric sector threat information is developed and used by critical asset owners, and how limitations and uncertainty of this information may affect physical security of the electric grid.

## Conclusion

The 2013 attack on the Metcalf transformer substation marked a turning point for the U.S. electric power sector. The attack prompted utilities across the country to reevaluate and restructure their physical security programs. It also set in motion proceedings in Congress and at FERC which resulted in the promulgation of NERC’s CIP-014 mandatory physical security standards in 2015. Based on discussions with FERC and NERC staff about utility compliance, as well as a review of public information about the activities of bulk power asset owners (and the vendors supplying them), there appear to be physical security improvements underway among owners of bulk power critical assets. The public record is too anecdotal to assert conclusively that these changes are occurring uniformly and at every relevant utility, but NERC’s summary compliance reports so far have been positive, especially for such a new standard. As NERC concluded in its *State of Reliability 2017* report,

What NERC can measure is that no major cyber- and few physical-related load losses have happened to date; that extremely low numbers of incidents have occurred on the

<sup>108</sup> NERC, *Compliance Monitoring and Enforcement Program Quarterly Report, Q3 2017*, November 8, 2017, p. 8.

<sup>109</sup> See, for example, Philip Shenon, “Threats and Responses: Domestic Security,” *New York Times*, June 5, 2003, p. A15.

<sup>110</sup> Deborah Carpentier, “NERC Gains in Vegetation Management, Cyber and Physical Security, and Reliability Assurance,” *Natural Gas & Electricity* (Wiley Periodicals), May 2014, p. 31, <http://www.crowell.com/files/NERC-Gains-in-Vegetation-Management-Cyber-and-Physical-Security-and-Reliability-Assurance.pdf>.

<sup>111</sup> Michael Chertoff, “Building a Resilient Power Grid,” *Electric Perspectives*, May/June 2014, p. 35.

operating side, and that attention to security performance has been excellent on the corporate side.<sup>112</sup>

Although the electric power sector seems to be moving in the direction of more extensive physical security, many measures have yet to be implemented and the process of corporate realignment around physical security is still underway. As the CPUC has stated,

It appears that the North American electric industry is in intermediate stages of fully harnessing the potential of security technologies and staff expertise, and integrating security and risk assessment values into the utility culture such that utility physical security ultimately is prioritized on par with safety and reliability.<sup>113</sup>

Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector's own assessments of risk. Bulk power physical security remains a work in progress. As CIP-014 implementation and other physical security initiatives proceed, Congress may seek to maintain its focus on the power sector's overall progress, not only on short term compliance with NERC's security standards, but also on structural changes supporting physical security as a priority far into the future.

## Author Contact Information

Paul W. Parfomak  
Specialist in Energy and Infrastructure Policy  
pparfomak@crs.loc.gov, 7-0030

---

<sup>112</sup> NERC, June 2017, p. 59.

<sup>113</sup> CPUC, January 2018, p. 57.





# NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?

**Paul W. Parfomak**

Specialist in Energy and Infrastructure Policy

March 19, 2018

**Congressional Research Service**

7-5700

[www.crs.gov](http://www.crs.gov)

R45135

## Summary

A 2013 rifle attack on a critical electric power substation in Metcalf, CA, marked a turning point for the U.S. electric power sector. The attack prompted utilities across the country to reevaluate and restructure their physical security programs. It also set in motion proceedings in Congress and at the Federal Energy Regulatory Commission (FERC) which resulted in a new mandatory *Physical Security Reliability Standard* (CIP-014) for bulk power asset owners promulgated by the North American Electric Reliability Corporation (NERC) in 2015. In the three years since FERC approved this new standard, security risks to the power grid have become an even greater concern in the electric utility industry. Reflecting these ongoing security concerns, legislative proposals in the 115<sup>th</sup> Congress include provisions directed at power grid physical security. Congress also continues its oversight of grid security and implementation of NERC's security standards.

Three entities play key roles in standards oversight and support of implementation for bulk power physical security. NERC and FERC oversee implementation of the CIP-014 standards, while the Department of Energy plays a supporting role in helping bulk power asset owners to protect their critical infrastructure. The detailed findings of NERC's compliance activities are not publicly disclosed due to their confidential nature. However, NERC has stated that the utility industry is making progress towards effective implementation of the CIP-014 standard and NERC has been "encouraged" by grid security measures put in place so far. NERC compliance audits as of February 2018 have uncovered no major failures to date.

In addition to compliance with NERC's standards, there have been other observable changes within the electricity sector reflecting greater emphasis on bulk power physical security. These changes include realignment in corporate structure to support physical security, incorporating physical security in transmission planning, new security products and services, utility capital investment in physical security, and utility participation in voluntary security programs. While public information about such changes is limited, it suggests they may be significant and widespread.

Although the electric power sector seems to be moving in the overall direction of greater physical security for critical assets, many measures have yet to be implemented and the process of corporate realignment around physical security is still underway. NERC's CIP-014 standards have been promulgated recently, and bulk power asset owners have largely begun enhancing physical security under the standard over the last two years. Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector's own assessments of risk. Bulk power security remains a work in progress.

Congress continues to be concerned about the current state of electric grid physical security. Among many specific issues of potential interest, Congress may focus on several with policy significance: security implementation oversight, cost recovery, hardening vs. resilience, and the quality of threat information. As CIP-014 implementation and other physical security initiatives proceed, Congress also may seek to maintain its focus on the power sector's overall progress, not only on short term compliance with NERC's security standards, but also on structural changes supporting physical security as a priority far into the future.

## Contents

Introduction .....	1
Power Grid Threat Environment .....	2
NERC's Physical Security Standards .....	3
Physical Security Standard Requirements.....	4
Federal Oversight and Support.....	4
NERC's Implementation Oversight .....	5
Electricity Information Sharing and Analysis Center .....	6
FERC Oversight.....	7
DOE Initiatives.....	8
Observed Changes in Bulk Power Physical Security .....	9
Corporate Structure Supporting Physical Security.....	9
Physical Security in Long-Term Transmission Planning .....	11
New Security Products and Services.....	12
Capital Investment in Physical Security.....	13
Utility Participation in Voluntary Security Programs.....	14
NERC Grid Security Exercises.....	14
DHS Critical Infrastructure Surveys .....	15
Legislative Proposals in the 115 <sup>th</sup> Congress .....	15
Policy Issues for Congress.....	16
Oversight of Physical Security Implementation.....	17
Financial Requirements and Cost Recovery .....	18
Hardening vs. Resilience.....	18
Threat Information .....	19
Conclusion.....	20

## Contacts

Author Contact Information .....	21
----------------------------------	----

## Introduction

Securing the electric power grid is among the highest priorities for critical infrastructure protection in the United States. In the past, power grid facilities have had varying degrees of access control and surveillance depending upon the facility type and location. These measures were largely focused on public safety (reflecting liability concerns) and preventing vandalism and theft. More recently, federal agencies, Congress, and the utility industry have focused greater attention on the vulnerability of the power grid, especially the high voltage transmission (bulk power) system, to terrorist attacks which could cause widespread, extended blackouts.

Until 2013, the emphasis of analysts and policymakers was on power grid cybersecurity—protecting the computer controls and communication systems used to operate the grid. However, a 2013 rifle attack on an electric transmission substation in Metcalf, CA, shifted more attention to the physical security of power grid critical assets. In response to the Metcalf attack, as well as other grid incidents and findings from utility security exercises, Congress passed new legislation to strengthen power grid physical security and to facilitate recovery in the event of a successful attack.<sup>1</sup> Congress also sought stronger physical security standards from the Federal Energy Regulatory Commission (FERC) under the commission’s existing statutory authority to regulate the reliability of the bulk power system. FERC, in turn, ordered the North American Electric Reliability Corporation (NERC)—the not-for-profit organization responsible for ensuring grid reliability—to promulgate new requirements for the physical security of bulk power critical infrastructure.<sup>2</sup> After consultation within the utility industry, NERC proposed new physical security standards in May 2014. FERC approved them, with minor changes, the following November.<sup>3</sup>

Since 2014, security risks to the power grid have become an even greater concern in the electric utility industry. Addressing them has remained a concern of Congress.<sup>4</sup> An emphasis on physical risk to the power grid was underscored in September 2016 by another successful rifle attack on a transformer substation—in Utah. Reflecting ongoing security concerns, legislative proposals in the 115<sup>th</sup> Congress include provisions directed at power grid physical security. Congress also continues its oversight of FERC’s grid security activities and the implementation of NERC’s physical security standards.

This report examines changes to the physical security of the electric power grid since the promulgation of NERC’s physical security standards. The report discusses the current risk environment for the bulk power system. It summarizes the key requirements of NERC’s security standards, including its applicability to specific assets, implementation deadlines, and oversight. The report reviews observable changes in the utility sector related to physical security. It concludes with an overview of proposed legislation and a discussion of policy issues for Congress.

---

<sup>1</sup> The Fixing America’s Surface Transportation (FAST) Act (P.L. 114-94), which became law on December 4, 2015, contains provisions to protect or restore the reliability of critical electric infrastructure or defense of critical electric infrastructure during a grid security emergency (§1104).

<sup>2</sup> Among other functions, NERC develops and enforces reliability standards, monitors the grid, and trains industry personnel. In the United States, NERC is subject to Federal Energy Regulatory Commission oversight.

<sup>3</sup> For more historical background and details regarding the development of NERC’s standards, see CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak.

<sup>4</sup> See for example: Senator Ron Johnson, Chairman, Opening statement before the Senate Committee on Homeland Security and Governmental Affairs hearing on “Threats to the Homeland,” September 27, 2017.

This report focuses primarily on physical security efforts to prevent successful physical attacks on the bulk power system. For analysis of issues specifically related to power grid cyberattacks and cybersecurity, see CRS Report R43989, *Cybersecurity Issues for the Bulk Power System*, by Richard J. Campbell. This report also does not address issues related to security incident recovery or restoration, except in the context of preventive physical security.

## Power Grid Threat Environment

Grid security analysts and policymakers have long been aware of physical risks to bulk power critical infrastructure, especially to high voltage (HV) transformer stations and substations, which serve as key nodes within the electric transmission system.<sup>5</sup> The 2013 Metcalf attack, in which an unknown perpetrator firing a .30 caliber rifle disabled a critical 500 kilovolt (kV) transformer substation, demonstrated that such facilities face real and potentially sophisticated threats.<sup>6</sup> The September 2016 rifle attack on a 69 kV transformer substation in Utah—which reportedly left 13,000 rural customers without power for up to eight hours—showed that similar incidents could occur almost anywhere on the grid.<sup>7</sup> A successful cyberattack on Ukraine’s power grid in 2015, which was reportedly attributed to Russian hackers, showed that foreign entities could view power grids as attractive targets.<sup>8</sup> A 2017 report from the National Academy of Sciences concludes: “While to date there have been only minor attacks on the power system in the United States, large-scale physical destruction of key parts of the power system by terrorists is a real danger. Some physical attacks could cause disruption in system operations that last for weeks or months.”<sup>9</sup>

The persistent threat environment has been changing the perception of physical threats among power grid owners and operators. For example, surveys of electric utility employees show that their physical (and cyber) security concerns are growing.<sup>10</sup> Exelon Corporation, one of the nation’s largest utility holding companies, stated in its 2016 annual report:

Threat sources continue to seek to exploit potential vulnerabilities in the electric...utility industry associated with protection of sensitive and confidential information, grid infrastructure and other energy infrastructures, and such attacks and disruptions, both physical and cyber, are becoming increasingly sophisticated and dynamic....The risk of these system-related events and security breaches occurring continues to intensify....<sup>11</sup>

Xcel Energy, another major utility owner, likewise states in its 2016 annual report:

---

<sup>5</sup> See, for example: National Research Council, *Terrorism and the Electric Power Delivery System*, 2012 and Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, June 1990.

<sup>6</sup> RTO Insider, “Substation Saboteurs ‘No Amateurs,’” April 2, 2014, <http://www.rtoinsider.com/pjm-grid2020-1113-03/>.

<sup>7</sup> Pat Reavy, “Power Company Offers Rare \$50K Reward for Information on Vandalism,” *Deseret News*, September 29, 2016. A substation rated at 69 kilovolts is not considered a “high voltage” transmission asset, although it may still serve large numbers of customers.

<sup>8</sup> Jim Finkle, “U.S. Firm Blames Russian ‘Sandworm’ Hackers for Ukraine Outage,” *Reuters*, January 7, 2016. The attack reportedly cut power to 80,000 customers for about six hours.

<sup>9</sup> National Academy of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation’s Electricity System*, 2017, p. 65, <https://doi.org/10.17226/24836>.

<sup>10</sup> Utility DIVE, *2017 State of the Electric Utility Survey*, April 10, 2017, [https://s3.amazonaws.com/dive\\_assets/rlpsys/SEU\\_2017.pdf](https://s3.amazonaws.com/dive_assets/rlpsys/SEU_2017.pdf).

<sup>11</sup> Exelon Corporation, *Annual Report Pursuant to Section 13 or 15(d) of the Securities and Exchange Act of 1934 for the Fiscal Year Ended December 31, 2016*, Form 10-K, February 13, 2017, p. 63.



Our generation plants, fuel storage facilities, transmission and distribution facilities and information systems may be targets of terrorist activities... The potential for terrorism has subjected our operations to increased risks and could have a material effect on our business.<sup>12</sup>

Accordingly, electricity sector-wide security exercises conducted by NERC have simulated attacks on power grid critical assets combining both cyber and physical dimensions.<sup>13</sup> These exercises are further discussed later in this report.

## NERC's Physical Security Standards

On March 7, 2014, FERC ordered NERC to submit proposed reliability standards requiring transmission owners meeting certain criteria “to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation” of the power grid.<sup>14</sup> In its order FERC stated that physical security standards were necessary because “the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks.”<sup>15</sup> According to the FERC order, the new reliability standards were to require transmission owners or operators to perform a risk assessment of their systems to identify “critical facilities,” evaluate the potential threats and vulnerabilities to those identified facilities, and develop and implement a security plan designed to protect against physical attacks on those identified critical facilities.<sup>16</sup> The order required that each of these steps be verified by NERC or another third party qualified to review them.

On May 23, 2014, NERC filed with FERC its proposal for mandatory physical security standards.<sup>17</sup> On November 20, 2014, FERC approved the proposed standard, with minor changes, as NERC's new *Physical Security Reliability Standard* (CIP-014-1).<sup>18</sup> Following publication in the *Federal Register*, FERC's order approving the standard became effective on January 26, 2015.<sup>19</sup> FERC approved a revised version of the standard (CIP-014-2) on July 14, 2015.<sup>20</sup> Required compliance for the standard began on October 1, 2015 with completion of the final parts required by November 24, 2016 for all applicable entities.

<sup>12</sup> Excel Energy, Inc. *Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2016*, Form 10-K, p. 44.

<sup>13</sup> North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014 and *Grid Security Exercise, GridEx III Report*, March 2016; Scott Heffentrager, PJM Interconnection, “GridEx IV Summary,” slide presentation, November 27, 2017, <http://www.pjm.com/-/media/committees-groups/committees/mc/20171127-webinar/20171127-item-04-2017-gridex-iv-summary.ashx>.

<sup>14</sup> Federal Energy Regulatory Commission (hereinafter, FERC), *Reliability Standards for Physical Security Measures*, Order Directing Filing of Standards, Docket No. RD14-6-000, March 7, 2014, p.1, <http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf>.

<sup>15</sup> FERC, March 7, 2014, p. 2.

<sup>16</sup> FERC, March 7, 2014, pp. 3-4.

<sup>17</sup> NERC, Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-014-1, May 23, 2014, <http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Physical%20Security%20CIP-014-1.pdf>.

<sup>18</sup> FERC, “Physical Security Reliability Standard,” Docket No. RM14-15-000, Order No. 802, November 20, 2014.

<sup>19</sup> NERC, “Physical Security Reliability Standard Implementation,” January 16, 2015, [http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20\(Agenda%20Excerpt\).pdf](http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20(Agenda%20Excerpt).pdf).

<sup>20</sup> FERC, letter order to the North American Electric Reliability Corporation, Docket No. RD-15-4-000, July 14, 2015, [http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Letter\\_Order\\_CIP-014\\_20150714\\_RD15-4.pdf](http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Letter_Order_CIP-014_20150714_RD15-4.pdf).

## Physical Security Standard Requirements

The stated purpose of NERC’s physical security reliability standard is “to identify and protect transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or cascading within an interconnection.”<sup>21</sup> It applies to transmission owners with assets operating at 500 kV or higher as well as owners with substations operating between 200 kV and 499 kV if they meet certain interconnection or load-carrying criteria.<sup>22</sup> The standard, generally referred to as “CIP-014,” consists of six principal requirements (R1-R6), summarized as follows:

- R1. Risk assessments by transmission owners to identify critical transmission facilities;
- R2. Independent third party verification of risk assessments conducted under R1;
- R3. Requirement for transmission owners with critical facilities identified under R1 but not under their operational control to notify the transmission operator of these facilities;<sup>23</sup>
- R4. Mandatory threat and vulnerability assessments for critical facilities conducted by transmission owners and operators;
- R5. Development, documentation, and implementation of physical security plans to protect critical facilities; and
- R6. Independent third party review of the threat and vulnerability assessments performed under R4 and security plans developed under R5.<sup>24</sup>

The standard also lays out a process for compliance monitoring and assessment including audits, self-certifications, spot checking, violation investigations, self-reporting, and handling complaints.<sup>25</sup> The new standard is enforced by NERC or another Regional Entity under a penalty review policy for mandatory reliability standards approved by FERC subject to the Commission’s enforcement authority and oversight under the Energy Policy Act of 2005 (P.L. 109-58).<sup>26</sup> Monitoring of compliance with the standard is further discussed below.

## Federal Oversight and Support

Three entities play key roles in standards oversight and implementation support for bulk power physical security. NERC and FERC directly oversee implementation of the CIP-014 standards, while the Department of Energy (DOE) plays a supporting role in helping bulk power asset owners to protect their critical assets.

---

<sup>21</sup> NERC, *CIP-014-2 – Physical Security*, printed December 5, 2017, p. 1, available at [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical%20Security&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical%20Security&jurisdiction=United%20States). (Hereinafter CIP-014-2). This report uses the terms “critical assets” and “critical substations” to mean “critical transmission stations and transmission substations” as defined under the CIP-014 standard.

<sup>22</sup> CIP-014-2.

<sup>23</sup> A regional transmission operator (RTO) administers the transmission grid for multiple transmission owners in a specified region in accordance with FERC Order No. 2000. RTOs and independent system operators (ISOs) are defined in Section 3 of the Federal Power Act (16 U.S.C. 796).

<sup>24</sup> CIP-014-2, pp. 3-6.

<sup>25</sup> CIP-014-2, p.8.

<sup>26</sup> FERC, *Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672*, Docket Nos. AD08-6-000 and RM05-30-002, April 17, 2008.

## NERC's Implementation Oversight

As stated above, with oversight by FERC, NERC has the authority to develop, oversee, and enforce implementation of the CIP-014 physical security standard.<sup>27</sup> NERC carries out these functions together with the eight Regional Entities (e.g., Midwest Reliability Organization) with which NERC has agreements to delegate its authority to monitor and enforce reliability standards compliance.<sup>28</sup> Collectively, NERC and the Regional Entities comprise the Electric Reliability Organization (ERO) Enterprise.

In general, NERC employs a risk-based framework to monitor compliance of all its grid reliability standards on the belief that monitoring and enforcement must be “right-sized” based on considerations including risk factors and management practices related to detecting, assessing, mitigating, and reporting of noncompliance.<sup>29</sup>

As reliability risk is not the same for all registered entities, the Framework examines [bulk power system] risk of registered entities both collectively and individually, to determine the most appropriate [Compliance Monitoring and Enforcement Program] tool to use when monitoring a registered entity's compliance with NERC Reliability Standards. The Framework also promotes an examination into how registered entities operate and tailor compliance monitoring focus to areas that pose the greatest risk to [bulk power system] reliability.<sup>30</sup>

NERC's approach offers flexibility in both the frequency and type of compliance monitoring (e.g., offsite or onsite audits, spot checks, or self-certifications) applied to an entity under a particular standard based on its particular level of reliability risk.<sup>31</sup> To support its compliance approach, NERC may conduct various activities, such as publishing guidance documents, providing training, and conducting outreach, “to promote transparency and confidence” in the utility industry's implementation of a standard.<sup>32</sup>

In monitoring compliance of the CIP-014 standard, NERC's focus in 2015 and 2016 was on the standards' requirements to identify critical transmission stations and substations (Requirements R1 and R2), ensuring that this identification was “appropriate and risk-informed.”<sup>33</sup> NERC required covered entities to self-certify with respect to: risk-assessment, identifying critical assets, and third party verification. NERC also conducted voluntary outreach through on-site visits with 19 covered entities to discuss security measures and CIP-014 implementation challenges.<sup>34</sup> In

<sup>27</sup> NERC's authorities to monitor compliance with its reliability standards and impose financial penalties are found in FERC regulations at 18 C.F.R. 39.7.

<sup>28</sup> See NERC, “Key Players,” web page, March 13, 2018, <http://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>.

<sup>29</sup> NERC, *Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program*, September 5, 2014, p. iv.

<sup>30</sup> NERC, *2017 ERO Enterprise Compliance Monitoring and Enforcement Implementation Plan, Version 2.5*, May 2017, p. 3.

<sup>31</sup> NERC, May 2017, p. 3.

<sup>32</sup> NERC, “Physical Security Reliability Standard Implementation,” January 16, 2015, p. 3, [http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20\(Agenda%20Excerpt\).pdf](http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20(Agenda%20Excerpt).pdf)

<sup>33</sup> NERC, May 2017, p. 16.

<sup>34</sup> NERC, *2016 ERO Enterprise Compliance Monitoring and Enforcement Program Annual Report*, February 8, 2017, p. 18, <http://www.nerc.com/pa/comp/CE/Compliance%20Violation%20Statistics/2016%20Annual%20CMEP%20Report.pdf>.

cases where there have been discrepancies between utility-generated critical asset lists and critical assets identified by the independent third parties, NERC has required the covered entities to provide further information and explanation to address the discrepancy. NERC has also been conducting audits of entities which have identified more, or fewer, critical substations as a percentage of all their substations than is typical.<sup>35</sup> The detailed findings of NERC's compliance activities are not publically disclosed due to the confidential nature of security information. However, NERC stated that, based on observations in 2016, the utility industry was "making progress towards effective implementation of and compliance with CIP-014-2."<sup>36</sup> A NERC presentation about its voluntary and informal site visits reported "remarkable progress" on physical security among 19 asset owners visited as of February 2016.<sup>37</sup>

In 2017, NERC increased its focus on the scope of utility security plans (R5), including their timelines for implementing security measures and the utility industry's overall progress in implementing CIP-014. The ERO Enterprise has prioritized auditing the quality of covered entities' risk management plans. In the second quarter of 2017, compliance audit staff were provided with guidance and training on bulk power physical security best practices as a reference for evaluating the physical security measures implemented by the covered entities.<sup>38</sup>

The ERO Enterprise expects to complete audits of the largest entities within three years of the effective date of CIP-014. As of February 2018, NERC had conducted compliance audits of approximately 45% of the covered entities with critical transmission stations and substations as defined under CIP-014. NERC had also audited over 30% of entities that did not identify critical assets after applying the CIP-014 criteria (under R1). NERC staff expects to have audited approximately 70% of the entities with CIP-014 critical assets by the end of 2018.<sup>39</sup> According to its stated schedule, NERC would audit the remaining entities in 2019. Subsequent monitoring and enforcement will focus more heavily on implementation of measures in the grid security plans.

According to NERC, the audits completed to date have not uncovered any major compliance failures, and NERC has been "encouraged" by security measures that utilities have put in place so far.<sup>40</sup> NERC has found no serious risk violations of the CIP-014 standard. Of 19 noncompliance issues identified, 8 were found to be "minimal" or "moderate" risk, with 2 warranting a financial penalty. The remaining 11 noncompliance issues are under review.<sup>41</sup>

## Electricity Information Sharing and Analysis Center

In addition to its standards activities, NERC also supports security of the electric power sector as the operator of the Electricity Information Sharing and Analysis Center (E-ISAC). Established in

<sup>35</sup> NERC, Staff meeting with CRS analysts, Washington, DC, December 7, 2017.

<sup>36</sup> NERC, May 2017, p. 16.

<sup>37</sup> Carl Herron, NERC, "CIP-014-02 Physical Security Site Visits," slide presentation, April 14, 2016, [https://www.frc.com/Compliance/EducationalMaterials/Educational%20Materials/Workshops%20-%20Workshop%20Event%20Materials/2016-04%20-%20OP%20Spring%20Compliance%20Workshop%20\(April%202012-14\)/7.%20CIP-014-2%20Physical%20Security%20Site%20Visits.pdf](https://www.frc.com/Compliance/EducationalMaterials/Educational%20Materials/Workshops%20-%20Workshop%20Event%20Materials/2016-04%20-%20OP%20Spring%20Compliance%20Workshop%20(April%202012-14)/7.%20CIP-014-2%20Physical%20Security%20Site%20Visits.pdf).

<sup>38</sup> NERC, *Compliance Monitoring and Enforcement Program Quarterly Report, Q2 2017*, August 9, 2017, p. 8, <http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/Compliance%20Committee%20Open%20Meeting%20-%20August%209%202017.pdf>.

<sup>39</sup> NERC, email to CRS, February 14, 2018.

<sup>40</sup> NERC, December 7, 2017.

<sup>41</sup> NERC, February 14, 2018.

1998, the E-ISAC is the electricity sector's primary communications channel for security-related information, situational awareness, incident management, and coordination.<sup>42</sup> Among its key responsibilities, the E-ISAC gathers and analyzes security data, shares it with stakeholders, and communicates security risk mitigation strategies.<sup>43</sup> Bulk power entities are required to report physical security events to the E-ISAC under NERC's Event Reporting Reliability Standard (EOP-004), which was approved by FERC in 2013 and revised in 2015.<sup>44</sup>

Although operated by NERC, the E-ISAC is independent and organizationally separate from NERC's standards enforcement functions; information shared by utilities with the E-ISAC is not passed on to NERC compliance staff.<sup>45</sup> Nonetheless, the E-ISAC has played a role in facilitating industry understanding of physical security best practices. For example, the E-ISAC has added significant physical security threats and tactics to the NERC's biennial GridEx security exercises (discussed later in this report). In 2015, the E-ISAC also established a Physical Security Advisory Group, which includes industry physical security professionals, outside experts, and representatives from DOE and the Department of Homeland Security (DHS), to assist in the analysis of physical security threats and advise asset owners on physical threat mitigation. Through these efforts, the E-ISAC developed and ratified a design basis threat for the electric sector in December 2015.<sup>46</sup> The E-ISAC also has hosted two threat workshops, with plans for more.<sup>47</sup> Thus, while the E-ISAC has had no role in enforcing the CIP-014 standards, the security risk and mitigation information it develops and promulgates support the activities of bulk power asset owners complying with the standards.

## FERC Oversight

As the agency with general statutory authority over grid reliability, and the agency which ordered and approved NERC's CIP-014 standard, the Federal Energy Regulatory Commission also oversees implementation of the standard. In carrying out this oversight, FERC relies primarily on annual compliance reporting by NERC.<sup>48</sup> However the commission also conducts some independent compliance activities, and it also conducts some compliance activities in cooperation with NERC. For example, during the initial rollout of the CIP-014 standard in 2016, FERC staff coordinated with NERC staff in support of on-site visits to the covered entities discussed above.<sup>49</sup>

In its order approving CIP-014-01, the commission stated that NERC staff would submit to both the NERC Board of Trustees and FERC a report following implementation of requirements R1,

---

<sup>42</sup> ISACs for critical infrastructure sectors were established under Presidential Decision Directive 63, May 22, 1998. NERC operates the E-ISAC in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC). The ESCC, established in 2004 by companies in the electric power industry, coordinates policy-related activities involving the reliability and resilience of the sector, including physical and cyber infrastructure.

<sup>43</sup> NERC, *Understanding Your E-ISAC*, June 2016, p. 3.

<sup>44</sup> NERC, "EOP-004-3—Event Reporting," 2015, <http://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-3.pdf>.

<sup>45</sup> NERC, June 2016, p. 3.

<sup>46</sup> NERC, *State of Reliability 2016*, May 2016, p. 7.

<sup>47</sup> NERC, *State of Reliability 2017*, June 2017, p. 62.

<sup>48</sup> FERC, *Order on Electric Reliability Organization Reliability Assurance Initiative and Requiring Compliance Filing*, Docket No. RR15-2-000, p. 11, February 19, 2015, [http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/FERC\\_Order\\_Approving\\_Risk-Based\\_CMEP.pdf](http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/FERC_Order_Approving_Risk-Based_CMEP.pdf).

<sup>49</sup> NERC, May 2017, p. 16.



R2, and R3 about the scope, number, and characteristics of facilities identified as critical.<sup>50</sup> The order stated that

Based on the results reported by NERC, we expect Commission staff to audit a representative number of applicable entities to ensure compliance with Reliability Standard CIP-014-1. Depending on the audit findings, the Commission will determine if there is a need for any further action by the Commission including, but not limited to, directing NERC to develop modifications to Reliability Standard CIP-014-1 to provide greater specificity to the methodology for determining critical facilities.<sup>51</sup>

As of November 2, 2017, FERC had completed two audits of critical assets identified by covered entities (R1) and was in the process of conducting a third. These audits have involved technical review of utility regulatory documents by FERC engineers. According to FERC staff, the initial audits identified one issue of concern related to the interpretation of specific language in the standard regarding asset criticality.<sup>52</sup> In addition to NERC's annual reports, FERC receives from NERC periodic Notices of Penalty (NOP) to regulated entities for reliability standards violations. As of November 30, 2017, FERC received NOPs for two violations (apparently at the same utility) of the CIP-014 standard.<sup>53</sup>

## DOE Initiatives

Presidential Decision Directive 63 (PDD-63), issued during the Clinton Administration in 1998, established national policy for critical infrastructure protection from both physical and cyber threats.<sup>54</sup> PDD-63 established 15 critical infrastructure sectors. The Department of Energy was assigned responsibility for (1) the electric power, and (2) the oil and natural gas production and storage sectors. The George W. Bush Administration built on the work of PDD-63, superseding it in 2003 with Homeland Security Presidential Directive 7 (HSPD-7) on "Critical Infrastructure Identification, Prioritization, and Protection."<sup>55</sup> HSPD-7 again assigned to DOE (as a Sector-Specific Agency) responsibility for the energy sector—including electric power—as well as responsibility for being the federal coordinator for all critical infrastructure protection efforts.<sup>56</sup> The Obama Administration superseded HSPD-7 with Presidential Policy Directive 21 (PPD-21) on "Critical Infrastructure Security and Resilience" in 2013.<sup>57</sup> PPD-21 retained the Sector-Specific Agencies (SSAs) from HSPD-7, with DOE continuing as the SSA for the energy sector. Thus, DOE has had a supportive role in helping utilities to protect bulk power critical assets over the last two decades.

<sup>50</sup> FERC, *Physical Security Reliability Standard*, Docket No. RM14-15-000, Order No. 802, November 20, 2014, p. 23, <http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Final%20Rule%20on%20CIP-014-1.pdf>.

<sup>51</sup> FERC, Order No. 802, p. 24.

<sup>52</sup> FERC, Staff meeting with CRS analysts, Washington, D.C., November 2, 2017.

<sup>53</sup> NERC, *Enforcement and Mitigation*, "Searchable NOP Spreadsheet," web page, accessed December 12, 2017, <http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx>.

<sup>54</sup> National Security Council and National Security Council Records Management Office, "PDD-63—Critical Infrastructure Protection," *Clinton Digital Library*, May 20, 1998.

<sup>55</sup> George W. Bush White House Archives, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive/HSPD-7, December 17, 2003.

<sup>56</sup> For details about the roles of Sector-Specific Agencies, see Department of Homeland Security, "Sector-Specific Agencies," web page, July 11, 2017, <https://www.dhs.gov/sector-specific-agencies>.

<sup>57</sup> Barack H. Obama White House Archives, "Critical Infrastructure Security and Resilience," Presidential Policy Directive-21, February 12, 2013.

Until recently, DOE's power grid security activities were led by its Office of Electricity Delivery and Energy Reliability (OE) within the Office of the Under Secretary for Science and Energy. A 2008 OE report stated that "OE's mission is to advance technology—in partnership with industry, government, academia, and the public—to meet America's need for a reliable, efficient, and resilient electric power grid."<sup>58</sup> Although the office was primarily focused on grid cybersecurity, it did conduct activities related to power grid physical security, including analysis of large power transformer security, a substation security awareness campaign, and efforts to support and coordinate research and development for physical security.<sup>59</sup> On February 14, 2018, DOE announced that the Secretary of Energy was establishing a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to be led by an Assistant Secretary with responsibilities to help protect energy infrastructure from "from cyber threats, physical attack and natural disaster."<sup>60</sup> How this reorganization will affect DOE's activities in bulk power physical security remains to be seen.

## Observed Changes in Bulk Power Physical Security

Most grid security analysts consider the 2013 Metcalf substation attack to have been the "wake up call" which both changed electric sector attitudes toward grid physical security and motivated the promulgation of NERC's physical security regulations. Since that time, there have been a number of apparent changes within the electricity sector related to increasing bulk power physical security. It is not clear whether these changes have been driven more by changes in utility perceptions of grid threats or by NERC's mandatory security standards. Furthermore, there is currently no comprehensive accounting of changes in physical security throughout the sector. Nonetheless, anecdotal information in the public domain suggests that such changes may be significant and widespread. They are discussed in the following sections.

## Corporate Structure Supporting Physical Security

One criticism that arose in the wake of the Metcalf attack was that physical security management at Pacific Gas and Electric Company (PG&E, the Metcalf substation's owner) and at other utilities was not a centrally organized or well-supported function in corporate management. This lack of support limited the influence of security managers in corporate planning and financial decisions.<sup>61</sup> However, it appears that many utilities have been reconfiguring and elevating physical security functions within their corporate structures. For example, owners of transmission assets such as PG&E, American Electric Power, and Xcel Energy have appointed Chief Security Officers at senior levels responsible for managing both physical and cyber security risks company-wide.<sup>62</sup>

<sup>58</sup> Department of Energy, Office of Electricity Delivery and Energy Reliability (Hereinafter OE), *National SCADA Test Bed Program, Multi-Year Plan FY2008-2013*, January 2008, p. 7.

<sup>59</sup> Department of Energy, Energy Sector-Specific Plan, 2015, pp. 16, 27. For discussion of OE's cybersecurity activities, see CRS Report R44939, *Cybersecurity for Energy Delivery Systems: DOE Programs*, by Paul W. Parfomak, Chris Jaikaran, and Richard J. Campbell.

<sup>60</sup> U.S. Department of Energy, "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response," press release, February 14, 2018.

<sup>61</sup> See, for example: Tony Kovalesski, Liz Wagner, and Mark Villarreal, "Internal Memo Reveals PG&E Years Away from Substation Security," *NBC Bay Area*, April 5, 2106, <https://www.nbcbayarea.com/investigations/Internal-Memo-Reveals-PGE-Years-Away-from-Substation-Security-303833811.html>.

<sup>62</sup> PG&E Corp., "Bernard A. Cowens," web page, January 9, 2017, <http://www.pgecorp.com/corp/about-us/officers/> (continued...)

The senior security professional, typically at the vice president or director level, now has direct access to the [Chief Executive Officer] and company boards of trustees, often to supply situational awareness of physical and cybersecurity issues.... The electricity industry is quickly moving away from security as an “addition duty”.... [M]ost utilities today have dedicated security departments committed to the protection of company assets and personnel.<sup>63</sup>

Utilities are also centralizing and bolstering their physical security capabilities at the operational level. Between 2014 and 2017, for example, Xcel Energy consolidated and grew its staffing for the “Chief Security Officer class of services” from 47 to 63 employees.<sup>64</sup> According to the company’s regulatory filings,

the increase in average staffing levels.... was due to the need to correct a lack of resources to ensure adequate headcount to provide essential cyber and physical Enterprise Security services for Xcel Energy.... This increase in staffing demonstrates the emerging need that led to a stand-alone organization (i.e., the Chief Security Officer) to focus on Cyber Operations, Enterprise Resilience, Physical Security and Security Governance.<sup>65</sup>

Likewise, in response to the Metcalf attack, Dominion Energy established “a true cross-functional team with more than 100 people representing the entire Dominion organization,” to develop and implement a more comprehensive substation security program.<sup>66</sup> Such efforts appear to extend to major publicly owned utilities as well. For example, according to the head of the Western Area Power Administration (WAPA), one of four federal power marketing administrations,

WAPA’s approach to physical security.... began in 2013 with the consolidation of our Office of Security and Emergency Management across our five regions and the implementation of a sophisticated risk-based program in analyzing the threats and vulnerabilities to our substations.<sup>67</sup>

The Tennessee Valley Authority (TVA), which operates federally-owned hydroelectric and nuclear generation and associated transmission assets, recently closed a job posting for eight entry-level Inspectors, each to be “trained as a physical security specialist” to provide “comprehensive security services, including assessments of facilities to identify credible threats, and implementation and testing of countermeasures to mitigate risks.”<sup>68</sup>

---

(...continued)

company/bernard-cowens.page; American Electric Power, “AEP Names Partlow Vice President & Chief Security Officer,” press release, August 25, 2015; Xcel Energy, *Application of Southwestern Public Service Company for Authority to Change Rates*, Direct Testimony of Stephen J. Brown, filing with the Public Utility Commission of Texas, August 21, 2017, <https://www.xcelenergy.com/staticfiles/xe-responsive/Company/Rates%20&%20Regulations/Rate%20Cases/Brown-RR-Direct.pdf>.

<sup>63</sup> Brian Harrell, “The Modern Look of a Utility’s Chief Security Officer,” *CSO*, August 4, 2016, <https://www.csoonline.com/article/3101474/leadership-management/the-modern-look-of-a-utilitys-chief-security-officer.html>.

<sup>64</sup> Xcel Energy, *Application of Southwestern Public Service Company for Authority to Change Rates*, Update Testimony of Stephen J. Brown, September 27, 2017, p. 10, <https://www.xcelenergy.com/staticfiles/xe-responsive/Company/Rates%20&%20Regulations/Rate%20Cases/13%20-%20BrownRRUpdate.pdf>.

<sup>65</sup> Xcel Energy, August 21, 2017, p. 26.

<sup>66</sup> Bob McGuire, et al., “Substation Security Is More Than Just a Fence,” *T&D World*, September 28, 2015.

<sup>67</sup> Mark A. Gabriel, Administrator and Chief Executive Officer, Western Area Power Administration, “Physical and Cyber Threats,” *T&D World*, May 8, 2017. Power Marketing Administrations (PMAs) operate electric transmission systems and sell power generated by federally-owned hydroelectric dams across much of the United States.

<sup>68</sup> Tennessee Valley Authority, “Inspector I – 507038,” job posting, *Linked-in JOBS*, web page, posted January 17, 2018, accessed February 1, 2018, <https://www.linkedin.com/jobs/view/inspector-i-507038-at-tennessee-valley-> (continued...)

Some transmission owners are also specifically increasing their in-house intelligence capabilities in physical security, including recent postings for positions such as “Security Intelligence Specialist” and “Director—Corp Security Info & Intelligence.”<sup>69</sup> While the examples above are anecdotal, they would be consistent with what may be a trend among key grid owners to make physical security a better-organized and more influential corporate function. Not all utilities may be implementing such organizational changes, however.

## Physical Security in Long-Term Transmission Planning

Since NERC promulgated the CIP-014 standards, some utilities have begun to put a greater emphasis on bulk power physical security as a design consideration in long-term transmission system planning. This approach aligns with the California Public Utilities Commission’s recommendation in its 2018 report that, “there should be an emphasis on incorporating a menu of physical security strategies [into] any substation from the time of its inception.”<sup>70</sup> For example, Public Service Enterprise Group’s transmission planning criteria for its Long Island system in New York discusses the use of power system simulation tools for “various transmission system security and reliability studies.”<sup>71</sup> Commonwealth Edison’s transmission planning criteria includes a separate section on “security criteria” for system design which considers “severe low probability outage combinations” and seeks “to avoid cascading outages, instability, or widespread blackout.”<sup>72</sup> Such criteria could apply to both natural and man-made outages, but they are consistent with, and readily applied to, design considerations for enhanced physical security. American Electric Power (AEP) also has incorporated asset criticality as a design criterion in its transmission planning.

As a result of the revised NERC CIP standards, AEP now classifies all of its bulk electric system facilities based on the critical nature of the equipment to determine the level of security needed. This approach allows us to design security controls directly into new infrastructure from the start, building the costs into capital projects as needed. It also allows us to be more proactive with new and existing infrastructure while balancing risks with mitigation solutions.<sup>73</sup>

In its plans for a 2018 reliability-related upgrade at one its substations, Vermont Electric Power Company states that it “will also take the opportunity to make improvements to the physical security” of the substation.<sup>74</sup> According to NERC officials, based on security criteria, some

---

(...continued)

authority-578188690.

<sup>69</sup> American Transmission Company, “Security Intelligence Specialist,” job listing on *LinkedIn*, posted March 6, 2017, <https://www.linkedin.com/jobs/view/security-intelligence-specialist-at-american-transmission-552328921>; Avangrid, “Director—Corp Security Info & Intelligence,” job listing on *Glassdoor.com*, posted January 3, 2018, [https://www.glassdoor.com/job-listing/director-corp-security-info-intelligence-avangrid-JV\\_IC1148470\\_KO0,40\\_KE41,49.htm?jl=2630675613&utm\\_source=google\\_jobs&utm\\_medium=organic](https://www.glassdoor.com/job-listing/director-corp-security-info-intelligence-avangrid-JV_IC1148470_KO0,40_KE41,49.htm?jl=2630675613&utm_source=google_jobs&utm_medium=organic).

<sup>70</sup> CPUC, January 2018, p. 8.

<sup>71</sup> PSEG Long Island, “Transmission Planning Criteria,” accessed January 10, 2018, p. 5, <https://www.psegliny.com/files.cfm/TransmissionPlanningCriteria.pdf>.

<sup>72</sup> Commonwealth Edison Co., “Transmission Planning Criteria,” February 10, 2017, p. 10, <https://www.pjm.com/-/media/planning/planning-criteria/commonwealth-edison-planning-criteria.ashx?la=en>

<sup>73</sup> American Electric Power Corp., *2017 AEP Corporate Accountability Report*, “Cyber and Physical Security,” web page, May 25, 2017, <http://www.aepsustainability.com/about/security/cyber.aspx>.

<sup>74</sup> Vermont Electric Power Company, “East Avenue & Queen City Substation Improvement Project,” web page, accessed February 1, 2018, <https://www.velco.com/our-work/projects/project-east-avenue-queen-city-substation-improvement-project>.

utilities also have begun to consider new transmission interconnections not only to increase line capacity for bulk power flows, but also to reduce the criticality of particular transformer substations in congested areas by providing more transmission paths around them.<sup>75</sup>

## New Security Products and Services

As utilities have devoted greater organizational and financial resources towards power grid physical security, industry vendors have been offering more physical security products and services to meet sector demand. As one utility services company has observed, “we can expect plenty of innovation as manufacturers see new markets due to the new standards for physical security of critical substations.”<sup>76</sup> These offerings range from analytical services for security planning to physical products to harden physical assets. A comprehensive survey of such offerings is beyond the scope of this report, but the following examples illustrate the kinds of products now commercially available in the bulk power physical security market.

- **Security Program Planning and Implementation.** Engineering and security consulting firms have developed customizable programs specifically for power grid physical security review, planning, analysis, and implementation in compliance with the CIP-014 standards and utility-specific requirements.<sup>77</sup>
- **Anti-Intrusion Products.** Vendors have been marketing existing intrusion-related products specifically for use at bulk power critical facilities. These products include visual, acoustic, thermal radar, and electromagnetic systems for facility monitoring, intrusion detection, and response.<sup>78</sup>
- **Hardened Transformers and Components.** At least two major manufacturers have been marketing bulk power transformers with integrated ballistic shielding, or customizable plates to shield existing transformers.<sup>79</sup> Smaller manufacturers have also begun marketing hardened transformer components, such as composite bushings, for new and retrofit substation applications.<sup>80</sup>
- **Substation Perimeter Shielding.** A number of vendors have been marketing perimeter fencing and wall products specifically for visual and physical shielding of bulk power substations.<sup>81</sup> Most of these products are designed specifically to protect against rifle attacks such as the Metcalf attack.

---

<sup>75</sup> NERC, December 7, 2017.

<sup>76</sup> Southwire Company, “Protecting the Grid,” *T&D World*, sponsored content, May 15, 2017.

<sup>77</sup> See, for example: Burns & McDonnell, “Station Defender,” web page, January 30, 2018, <https://info.burnsmcd.com/station-defender/project-delivery>; Corporate Risk Solutions, “Physical Security,” web page, January 30, 2018, <https://corprisk.net/physical-security/>.

<sup>78</sup> See, for example: “How VTI Security Protected an Electrical Substation With a Radar-Thermal Imaging Solution,” *Security Sales & Integration*, September 20, 2017, <https://www.securitysales.com/in-depth/vti-security-radar-thermal-imaging-solution/>; and i2c Technologies, Ltd., “Power Substation Protection,” marketing brochure, May 2017, <http://www.i2ctech.com/wp-content/uploads/2017/05/2509-i2cTech-CMYK.pdf>.

<sup>79</sup> See, for example: Siemens AG, “First Bullet Resistant Retrofit Ordered for a Transformer,” press release, accessed January 28, 2018, <https://www.siemens.com/global/en/home/products/energy/references/first-bullet-resistant-retrofit-ordered-for-a-transformer.html>.

<sup>80</sup> Mike Sheppard and Saqib Saeed, “Bullet and Weather Concerns Driver of Retrofits in US Market,” Power Technology Research LLC, October 26, 2017, <https://powertechresearch.com/bullet-and-weather-concerns-driver-of-retrofits-in-us-market/>.

<sup>81</sup> See for example: Oldcastle, Inc., “How Precast Substation Walls Increase Power Grid Security,” web page, <https://www.buildingsolutions.com/industry-insights/how-precast-substation-walls-increase-power-grid-security>; (continued...)



Although new physical security products and services are being marketed in the utility sector, there is no comprehensive source of data about their sales to bulk power asset owners. Simply because vendors are marketing products does not mean that many utilities are buying them. For example, as of October 2017, Siemens Corp. had announced only one commercial order for its new transformer ballistic shielding retrofit product.<sup>82</sup> Thus, the overall impact of such offerings on the sector cannot be qualified reliably. Additional discussion of physical security spending is in the following section.

## Capital Investment in Physical Security

Major changes in power grid operational expenses and capital investment are generally slow to occur. In privately owned utilities, significant changes in spending and plans for new capital projects may need to go through a number of rigorous screens, including power network modeling, a corporate capital allocation process, a regulatory approval process, and a procurement process. Publicly owned utilities may need approval from cooperative boards, or municipal or federal officials. This combination of requirements can take years to complete. Consequently, many significant operating expenditures or capital investments for physical security identified in security plans under CIP-014 may still be working their way through utility budgets and implementation. For example, in a 2016 rate filing, Southern California Edison stated that it planned to make physical security improvements at approximately 24 facilities in 2015-2017 and proposed to upgrade 8 substations per year from 2016 through 2020.<sup>83</sup> Likewise, in its 2016 annual report, Dominion Resources' timeline for power grid capital investment in "Physical Security" runs to 2021.<sup>84</sup>

Notwithstanding the potential length of time it may take for some security projects to be approved and implemented, there are indications in the public record that bulk power asset owners have already been spending more on new physical security measures. In its December 2016 report, the Edison Electric Institute stated that "primary factors driving transmission investment between 2015 and 2019" included "system hardening and resiliency to minimize adverse catastrophic events" and "improvements to comply with evolving transmission reliability and security compliance standards."<sup>85</sup> In its January 2018 white paper, the California Public Utilities Commission (CPUC) reports that investor-owned utilities under its jurisdiction "already ... have sought approval for tens of millions of dollars in General Rate Case funding to ensure physical security."<sup>86</sup> The following examples illustrate the types of physical security projects and recent spending in publicly available sources.

---

(...continued)

AFTEC LLC, "Substation Security Walls," web page, 2017, <https://aftec.com/substation-security-walls/>;

<sup>82</sup> Siemens AG, "First Bullet Resistant Retrofit Ordered for a Transformer," press release, October 17, 2017, <https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/energy-management/medium-voltage-power-distribution/2017-10-17-tr-success-bullet-resistant-retrofit-v1-en.pdf>.

<sup>83</sup> Southern California Edison Co., Application Of Southern California Edison Company (U 338E) For Authority To Increase Its Authorized Revenues For Electric Service In 2018, Among Other Things, And To Reflect That Increase In Rates, A.16-09-001, Before the Public Utilities Commission of the State of California, September 1, 2016, [http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/9F664E3F0B77B7E488258195007C8F53/\\$FILE/SCE%20Opening%20Brief%20and%20COS.pdf](http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/9F664E3F0B77B7E488258195007C8F53/$FILE/SCE%20Opening%20Brief%20and%20COS.pdf).

<sup>84</sup> Dominion Resources, Inc., *Energy is Essential*, 2016 Summary Annual Report, 2017, p. 5.

<sup>85</sup> Edison Electric Institute, *Transmission Projects: At A Glance*, December 2016, p. vi.

<sup>86</sup> California Public Utilities Commission (CPUC), *Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699*, January 2018, p. 5.

- In 2017, the Bonneville Power Administration announced stand-alone plans to install security fencing at two high-voltage substations in compliance with NERC's security standards and to "protect critical assets from theft, vandalism, and terrorism."<sup>87</sup>
- In 2017, PPL Electric Utilities reportedly filed for regulatory approval for a \$450,000 expenditure to reconfigure a 500 kV substation in compliance with NERC's CIP-014 physical security standard.<sup>88</sup>
- In 2017 regulatory filings, Vectren (Indiana) described plans to invest \$2.9 million for physical security upgrades at critical substations, including enhanced fencing, access control, video surveillance, and perimeter motion detection.<sup>89</sup>
- According to the Western Area Power Administration, its expenses for physical security "nearly tripled" between 2013 and 2017.<sup>90</sup>

## Utility Participation in Voluntary Security Programs

Although the CIP-014 mandatory physical security standards have only been in effect since 2014, bulk power asset owners have had earlier opportunities to participate in voluntary security initiatives administered by NERC and DHS. Utility participation in these voluntary programs is another indication of overall efforts in the sector to improve critical asset physical security.

## NERC Grid Security Exercises

In 2011, NERC conducted GridEx, the first of an ongoing series of biennial electric sector-wide grid security exercises.<sup>91</sup> The 2011 exercise assessed the readiness of utilities to respond to a cyberattack, strengthened their crisis response, and provided input for internal security program improvements. Although the exercise was focused on a cyberattack, it did involve physical incursions into power grid substations as well as aspects of grid monitoring and recovery that would be relevant to an attack on critical transformers.<sup>92</sup> After the Metcalf attack in 2013, NERC conducted a second, more expansive grid security exercise, GridEx II. The exercise scenario included a cyberattack on the grid coupled with a coordinated physical attack against a subset of transmission and generation assets—including critical transformer substations.<sup>93</sup> NERC conducted GridEx III in 2015, again including a baseline scenario with cyber and physical

<sup>87</sup> Bonneville Power Administration, Categorical Exclusion Determination, "Proposed Action: Covington and Maple Valley Substations Perimeter Security Upgrades," April 27, 2017, [https://www.bpa.gov/efw/Analysis/CategoricalExclusions/cx/20170427\\_Covington-and-Maple-Valley-Substations-Perimeter-Security-Upgrades.pdf](https://www.bpa.gov/efw/Analysis/CategoricalExclusions/cx/20170427_Covington-and-Maple-Valley-Substations-Perimeter-Security-Upgrades.pdf).

<sup>88</sup> Corina Rivera Linares, "PPL Electric Utilities Seeks Approval of Two Projects in Pennsylvania," *Transmission Hub*, PennWell Publishing, May 22, 2017.

<sup>89</sup> Southern Indiana Gas and Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc. IURC Cause No. 44910, filing with the Indiana Utility Regulatory Commission, February 23, 2017, Attachment LKW-2, p. 31, [https://iurc.portal.in.gov/\\_entity/sharepointdocumentlocation/b4477c28-00fa-e611-8104-1458d04e8ff8/bb9c6bba-fd52-45ad-8e64-a444aef13c39?file=44910\\_Vectren%20South\\_No%202\\_Direct%20Testimony%20and%20Attachments\\_Wilson\\_PUBLIC\\_022317.pdf](https://iurc.portal.in.gov/_entity/sharepointdocumentlocation/b4477c28-00fa-e611-8104-1458d04e8ff8/bb9c6bba-fd52-45ad-8e64-a444aef13c39?file=44910_Vectren%20South_No%202_Direct%20Testimony%20and%20Attachments_Wilson_PUBLIC_022317.pdf)

<sup>90</sup> Mark A. Gabriel, May 8, 2017.

<sup>91</sup> NERC's E-ISAC division organizes and administers its GridEx exercises.

<sup>92</sup> North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. i.

<sup>93</sup> NERC, *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.15; Matthew L. Wald, "Attack Ravages Power Grid. (Just a Test.)," *New York Times*, November 14, 2013.

attacks, but also with an option for participants to customize the baseline scenario to meet local objectives.<sup>94</sup> NERC conducted its most recent exercises, GridEx IV, in November 2017.

According to NERC, one indication of progress in bulk power grid security is increasing participation by electricity sector entities in its GridEx exercises. The number of utilities participating in GridEx rose from 49 in 2011 to 166 in 2015.<sup>95</sup> NERC has not yet released participation details for GridEx IV, but the DOE reported that the latest exercise had more participants than in 2015.<sup>96</sup>

## DHS Critical Infrastructure Surveys

The Department of Homeland Security's Protective Security Coordination Division conducts voluntary field assessments of critical infrastructure to identify vulnerabilities, interdependencies, capabilities, and cascading effects of potential terrorist attacks. As part of these efforts, DHS Protective Security Advisors offer voluntary, web-based security surveys of critical facility security using the agency's Infrastructure Survey Tool developed in 2008. The key goals of the surveys are to identify facilities' physical security and security management, identify security gaps, create facility protective and resilience measures indices that can be compared to similar facilities, and track progress toward improving security.<sup>97</sup> According to DHS officials, of more than 6,000 surveys completed since the program began, over 600 have been conducted on electric power facilities—although the timing of these surveys and the specific types of power facilities involved are not reported.<sup>98</sup>

## Legislative Proposals in the 115<sup>th</sup> Congress

Given the relatively recent promulgation of NERC's new physical security standards, bulk power physical security has not been a major legislative focus in the 115<sup>th</sup> Congress. Nonetheless, several bills include provisions intended to enhance bulk power physical security—primarily by establishing new DOE grid security programs rather than by imposing new requirements on FERC or on bulk power asset owners directly. The relevant provisions of these bills, and a related resolution, are summarized below.

- **The Enhancing Grid Security Through Public-Private Partnerships Act** (H.R. 5240) would require DOE to establish a program to facilitate public-private partnerships for electric utility physical security and cybersecurity, among other provisions. Program activities would support voluntary implementation of maturity models, self-assessment, and security auditing; sharing of best practices and data collection in the electric sector; and training and technical assistance to utilities (§2(a)).

<sup>94</sup> NERC, *Grid Security Exercise: GridEx III Report*, March 2016, p. 7.

<sup>95</sup> NERC, March 2016, p. 1.

<sup>96</sup> U.S. Department of Energy, "GridEx IV: Government and Industry Exercise Together to Improve the Response to Grid Security Emergencies," November 21, 2017, <https://energy.gov/articles/gridex-iv-government-and-industry-exercise-together-improve-response-grid-security>.

<sup>97</sup> Department of Homeland Security, "Critical Infrastructure Vulnerability Assessments," web page, April 17, 2017, <https://www.dhs.gov/critical-infrastructure-vulnerability-assessments>.

<sup>98</sup> Daniel Genua, Department of Homeland Security, Presentation at George Mason University, Center for Energy Science and Policy, Grid Security Symposium, Arlington, VA, October 25, 2017, [http://cesp.gmu.edu/wp-content/uploads/2017/10/UNCLASS\\_GMU-Panel-Presentation\\_25Oct2017\\_FINAL.pdf](http://cesp.gmu.edu/wp-content/uploads/2017/10/UNCLASS_GMU-Panel-Presentation_25Oct2017_FINAL.pdf).

- The **Energy Emergency Leadership Act** (H.R. 5174) would amend the Department of Energy Organization Act to include “energy emergency and energy security” to the functions assigned to Assistant Secretaries. These functions would include responsibilities with respect to emerging threats, supply, and emergency planning, among others. They would also include “provision of technical assistance, support, and response capabilities with respect to energy security threats, risks, and incidents” (§2).
- The **Energy and Natural Resources Act of 2017** (S. 1460) would require DOE to develop an advanced energy security program to secure energy networks, including electric transmission and delivery. Eligible activities would include developing “capabilities to identify vulnerabilities and critical components that pose major risks to grid security if destroyed or impaired,” modeling national level impacts from human-made events, developing a physical security maturity model, conducting grid security exercises, conducting research on critical asset hardening, and other related measures (§2002(e)).
- The **Leading Infrastructure for Tomorrow’s America Act** (H.R. 2479) would establish a grant program administered by DOE “to enhance energy security through measures for electricity delivery infrastructure hardening and enhanced resilience and reliability” (§31101(a)).
- The **Advancing Grid Storage Act of 2017** (S. 1851) would establish a competitive grant program for pilot energy storage systems administered by DOE with one objective being to “improve the security of critical infrastructure and emergency response systems” in the electric grid (§5(a)(4)(A)).
- The **Grid Cybersecurity Research and Development Act** (H.R. 4120) would require DOE, together with bulk power asset owners, and in collaboration with the National Laboratories, to “utilize a range of methods, including voluntary vulnerability testing and red team-blue team exercises, to identify vulnerabilities in physical and cyber systems” (§6(a)).
- The **Flexible Grid Infrastructure Act of 2017** (S. 1875) would require DOE to: develop model standards for the electric distribution grid, in part to improve security with respect to physical threats (§5(d)(1)), evaluate whether new performance standards and testing procedures are needed to ensure electrical equipment resilience in the face physical threats (§5(d)(2)), and submit to Congress methods and guidelines for calculating the costs and benefits of investments in resilience and security solutions for the electric grid (§5(e)(1)).
- **House Resolution 334** states that it should be the policy of the United States to, among other things, “bolster the reliability, affordability, diversity, efficiency, security, and resiliency of domestic energy supplies, through advanced grid technologies,” and to promote advanced grid tools “to increase data security, physical security, and cybersecurity awareness and protection.”

## Policy Issues for Congress

Although NERC’s CIP-014 standards have been promulgated, and bulk power asset owners have begun enhancing physical security, Congress continues to be concerned about the current state of electric grid physical security. Among many issues of potential interest, Congress may focus on several with overarching policy significance: security implementation oversight, cost recovery, hardening vs. resilience, and the quality of threat information.

## Oversight of Physical Security Implementation

Although FERC's statutory authority for grid reliability and NERC's reliability standards both include provisions for oversight and enforcement, congressional oversight of physical security implementation may be a challenge for several reasons. First and foremost, information about physical security measures is inherently sensitive and there are both statutory and regulatory restrictions on its disclosure.<sup>99</sup> Therefore, the level of security-related information that utilities are willing or able to provide outside the CIP-014 third-party review process or NERC compliance audits is more limited than reports about, say, general reliability or safety.

NERC is not compiling a centralized database of critical assets or security measures implemented by the utilities subject to its physical security standard. Moreover, while NERC may provide security information to FERC, the security-related information NERC can provide in public reports is limited and typically redacted. Therefore, although information about CIP-014 implementation exists among the utilities and independent third parties (operating within the standard), and is provided at some level of specificity to NERC, that information may not be as useful or visible as it could be to Congress or other outside entities.

Another oversight challenge arises because NERC's CIP-014 standards are not prescriptive; bulk power asset owners have considerable discretion in the nature and timing of the physical security measures they may include in their physical security plans. NERC viewed such flexibility as necessary for its standard due to the unique characteristics of each utility's bulk power system and the risks it faces. However, this flexibility also may make it more difficult to develop useful metrics for CIP-014 implementation and comparing implementation among asset owners. NERC's standards for power grid physical security may ensure considerable consistency in the *process* utilities must undertake to identify critical substations and develop plans to secure them. However, they may not ensure consistency among the various security plans nor in the specific measures the individual asset owners will choose to implement to reduce the risk of intentional attacks. For example, ballistic shielding at critical substations may be an appropriate and sufficient protective measure for some utility assets, say, in open and rural areas, but not necessarily in more urban areas.

Even when detailed company-specific information about physical security measures is available, it might be difficult to develop reliable metrics to evaluate it. Metrics are an important tool NERC uses to evaluate utility performance in the context of power grid reliability.<sup>100</sup> However, officials at EEI have stated that measuring the adequacy of grid security for a diverse set of asset owners under changing risk circumstances poses significant problems. "Security metrics (for both cyber and physical security) have consistently been a challenge due evolving threats and vulnerabilities. If you build an eight-foot fence, the attacker just needs to bring a nine-foot ladder."<sup>101</sup> NERC is actively engaged in efforts to develop bulk power system security metrics in which it has likewise encountered "challenges associated with developing relevant and useful security metrics that rely on data willingly and ably provided by individual entities."<sup>102</sup>

---

<sup>99</sup> FERC regulations for the submission, designation, handling, sharing, and dissemination Critical Energy/Electric Infrastructure Information (CEII) are at 18 C.F.R. § 388.113.

<sup>100</sup> See NERC, "Reliability Indicators," web page, <http://www.nerc.com/pa/RAPA/Pages/ReliabilityIndicators.aspx>.

<sup>101</sup> Chris Hickling, Edison Electric Institute, "RE: CIP-014 Implementation Update," email to CRS, October 30, 2017.

<sup>102</sup> NERC, *State of Reliability 2017*, June 2017 p. vii. For an expansive discussion of NERC's efforts to develop security metrics, see Appendix G in this NERC report.



Congress may judge the effectiveness of the CIP-014 physical security standards as best it can based on reports and testimony from NERC and FERC as well as information from the assets owners themselves. However, due to the issues above, if Congress decides the information as currently structured is insufficient to draw reliable conclusions about the status of bulk power physical security as a whole, it may revisit how the responsible agencies collect, measure, and report it. Congress may also consider additional avenues for reviewing this information, for example, through classified briefings or specifically requested studies or reports. Also, as FERC continues to implement its policy of regulating physical security of the power grid, Congress may examine whether company-specific security initiatives appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid overall uniformly reflect terrorism risk from a national perspective.

## Financial Requirements and Cost Recovery

Two of the barriers to physical security investment among utilities prior to the Metcalf attack were competition for limited capital investment resources and justifying security spending to corporate boards and utility rate regulators. NERC regulatory requirements for physical security make it easier for security managers to justify related operating and capital expenditures to corporate leadership, and to seek cost recovery for such expenditures through regulated rates. However, even where regulators have been supportive of cost recovery for physical security investments in general, they have faced challenges gauging the prudence of specific security investments because they are hard to evaluate on a traditional benefit-cost basis. As a 2006 report from the Electric Power Research Institute states,

Security measures, in themselves, are cost items, with no direct monetary return. The benefits are in the avoided costs of potential attacks whose probability is generally not known. This makes cost-justification very difficult.<sup>103</sup>

Note that cost-justification requires not only the approval of utility management, but also of FERC and potentially state public utility commissions which regulate the rates grid owners may charge for electric transmission and distribution service. Regulators are responsible for ensuring that electricity rates are just and reasonable. They must be convinced that any new grid security capital costs and expenses are necessary and prudent before they will allow them to be passed through to ratepayers. However, corporate financial processes differ from utility to utility, and utility rate regulation differs from jurisdiction to jurisdiction, so investment and cost recovery for physical security is not uniform across the electricity sector and remains a work in progress. As implementation of new physical security plans under CIP-014 continues, Congress may examine whether the overall level of investment appropriately reflects the level of security risk facing the bulk power system, and whether any cost-recovery barriers are preventing assets owners from making investments necessary to secure the grid.

## Hardening vs. Resilience

There are two fundamental approaches to reducing the risk of a successful physical attack on the electric grid. The first approach, which is the principal approach of NERC's CIP-014 standards, is to prevent attacks by monitoring critical facilities to identify would-be attackers before they attempt an attack, preventing attacker access to critical assets, and otherwise hardening facilities

---

<sup>103</sup> Electric Power Research Institute (EPRI), *Technologies for Remote Monitoring of Substation Assets: Physical Security*, March 2006, p. viii.

to make them more physically secure to protect against attack and equipment failure. The second approach is to make the broader power system more “resilient” to a successful attack on particular assets through an enhanced ability to manage loads, reroute power flows, and access other sources of generation to reduce the potential of blackouts even if critical assets are disabled.<sup>104</sup> Initiatives such as the spare transformer program administered by the Edison Electric Institute (EEI, the electric utility trade association), and a proposed federal Strategic Transformer Reserve, which can accelerate replacement of critical transformers if they are damaged, may contribute to the power grid’s ability to sustain a terrorist attack without widespread grid failure.<sup>105</sup> Thus, while hardening is aimed more at reducing the likelihood of a successful attack, resilience aims at reducing potential consequence; doing either reduces overall security risk.

Measures to harden critical facilities and measures to increase system resilience are not exclusive of one another. In fact, they can be complementary in reducing overall security risk. However, they may involve different approaches to power grid operation and design, and they may involve different, competing types of investment (e.g., transformer shielding vs. transmission network sensors). Balancing the two approaches to most efficiently achieve a desired level of physical security is a challenge for utilities with limited capital budgets. The CPUC stated that “determining appropriate security measures or approaches to ensuring resiliency” was one of three “major issues” in its power grid physical security proceedings.<sup>106</sup> As Congress continues its oversight of bulk power physical security regulation, it may consider whether the electric power sector as a whole is striking an appropriate balance between these two approaches.

## Threat Information

The utility industry’s physical security risk assessments rely upon threat information from the federal government, among other sources.<sup>107</sup> The quality of this threat information is a key determinant of what bulk power asset owners need to be protecting against and what security measures to take. Incomplete or ambiguous threat information may lead to inconsistency in physical security among grid owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat.

As discussed earlier in this report, the E-ISAC plays a valuable role in identifying and analyzing physical security risk, and disseminating information about those risks to bulk power asset owners. Independent third-party verification of risk assessments under the CIP-014 standards, together with NERC compliance audits, are two additional means of helping to ensure greater consistency of threat information among utilities. Nonetheless, a changing threat environment continues to pose challenges for physical security planning and investment. As NERC stated in a

<sup>104</sup> For a discussion about power grid resiliency and associated federal efforts, see *Government Accountability Office, Electricity: Federal Efforts to Enhance Grid Resilience*, GAO-17-153, January 2017.

<sup>105</sup> For details about electric sector spare transformer programs, see Department of Energy, *Strategic Transformer Reserve*, report to Congress, March 2017.

<sup>106</sup> CPUC, January 2018, p. 5.

<sup>107</sup> Much of this information is communicated primarily through the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the sector’s communications channel for security-related information, situational awareness, incident management, and coordination. The ES-ISAC was established under Presidential Decision Directive 63, May 22, 1998. The ES-ISAC is operated by NERC in collaboration with the DOE and Electricity Subsector Coordinating Council. Members may anonymously share information by means of a secure Internet portal. Registered users receive information on security threats and alerts, remediation, task forces, events, and other security-specific resources.

recent compliance report, “the security threat landscape is constantly changing and requires adaptation and information sharing on how best to address these issues in an effective and efficient manner.”<sup>108</sup>

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.<sup>109</sup> Threat information continues to be an uncertainty in the case of power grid physical security. For example, although there is wide consensus that the Metcalf attack was extremely alarming, some industry analysts have opined that FERC’s physical security order nonetheless may have been an “overreaction” to Metcalf.<sup>110</sup> By contrast, former DHS Secretary Michael Chertoff has predicted that “the sophistication and resulting damage of the Metcalf attack will ... be exceeded” in a future attack.<sup>111</sup> Still others have expressed concern that FERC’s physical security concerns may be too heavily focused on another Metcalf-type scenario—the last threat—rather than a wider range of potential future threats.

As discussed earlier, there is widespread belief that bulk power critical assets are vulnerable to physical attack, that such an attack potentially could have catastrophic consequences, and that the risks of such attacks are growing. But the exact nature of such potential attacks and the capability of perpetrators to successfully execute them are uncertain. Consequently, despite the technical arguments, with limited information about potential targets and attacker capabilities, the true vulnerability of the grid remains an open—and evolving—question. As Congress seeks to establish the best policies to address bulk power physical security, it may examine how federal and electric sector threat information is developed and used by critical asset owners, and how limitations and uncertainty of this information may affect physical security of the electric grid.

## Conclusion

The 2013 attack on the Metcalf transformer substation marked a turning point for the U.S. electric power sector. The attack prompted utilities across the country to reevaluate and restructure their physical security programs. It also set in motion proceedings in Congress and at FERC which resulted in the promulgation of NERC’s CIP-014 mandatory physical security standards in 2015. Based on discussions with FERC and NERC staff about utility compliance, as well as a review of public information about the activities of bulk power asset owners (and the vendors supplying them), there appear to be physical security improvements underway among owners of bulk power critical assets. The public record is too anecdotal to assert conclusively that these changes are occurring uniformly and at every relevant utility, but NERC’s summary compliance reports so far have been positive, especially for such a new standard. As NERC concluded in its *State of Reliability 2017* report,

What NERC can measure is that no major cyber- and few physical-related load losses have happened to date; that extremely low numbers of incidents have occurred on the

<sup>108</sup> NERC, *Compliance Monitoring and Enforcement Program Quarterly Report, Q3 2017*, November 8, 2017, p. 8.

<sup>109</sup> See, for example, Philip Shenon, “Threats and Responses: Domestic Security,” *New York Times*, June 5, 2003, p. A15.

<sup>110</sup> Deborah Carpentier, “NERC Gains in Vegetation Management, Cyber and Physical Security, and Reliability Assurance,” *Natural Gas & Electricity* (Wiley Periodicals), May 2014, p. 31, <http://www.crowell.com/files/NERC-Gains-in-Vegetation-Management-Cyber-and-Physical-Security-and-Reliability-Assurance.pdf>.

<sup>111</sup> Michael Chertoff, “Building a Resilient Power Grid,” *Electric Perspectives*, May/June 2014, p. 35.

operating side, and that attention to security performance has been excellent on the corporate side.<sup>112</sup>

Although the electric power sector seems to be moving in the direction of more extensive physical security, many measures have yet to be implemented and the process of corporate realignment around physical security is still underway. As the CPUC has stated,

It appears that the North American electric industry is in intermediate stages of fully harnessing the potential of security technologies and staff expertise, and integrating security and risk assessment values into the utility culture such that utility physical security ultimately is prioritized on par with safety and reliability.<sup>113</sup>

Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector's own assessments of risk. Bulk power physical security remains a work in progress. As CIP-014 implementation and other physical security initiatives proceed, Congress may seek to maintain its focus on the power sector's overall progress, not only on short term compliance with NERC's security standards, but also on structural changes supporting physical security as a priority far into the future.

## Author Contact Information

Paul W. Parfomak  
Specialist in Energy and Infrastructure Policy  
pparfomak@crs.loc.gov, 7-0030

---

<sup>112</sup> NERC, June 2017, p. 59.

<sup>113</sup> CPUC, January 2018, p. 57.